Latest amended version March 2012

Amendments in July 2004 were made to:
- Collection Notices pages 20 - 22
- Draft Privacy Policies, Annexure A: page 4 in each case
- Part 3, Section 16 (A): School Counsellors and Privacy and Protected Confidences for victims of sexual assault
- Part 4, Section 18: Health Records Legislation in NSW, ACT, Victoria

Amendments in July 2007 were made to:
- Part 2, Section 7: Collection through monitoring of computer use
- Part 2, Section 7: Collection of information about prospective students [NSW only]
- Part 2, Section 8: Disclosure authorised by law in NSW
- Part 3, Section 16: School counsellors and privacy
- Part 3, Section 16: Passing personal information to other Schools
- Part 3, Section 16: Disclosure of information in NSW
- Annexure B: Email and Internet Policy

Amendments in December 2011 were made to:
- Part 7, Section 10: Standard Collection Notice - MySchool

Amendments in March 2012 were made to:
- Part 7, Section 10: Standard Collection Notice – Cloud Computing

NATIONAL CATHOLIC EDUCATION COMMISSION AND
NATIONAL COUNCIL OF INDEPENDENT SCHOOLS' ASSOCIATIONS

PRIVACY COMPLIANCE MANUAL

This Manual may be used by schools and systems which are represented by the Catholic Education Commission and by schools which are Members of an Association of Independent Schools.

11 DECEMBER 2001 (Latest amended version March 2012)

Minter Ellison Lawyers
Aurora Place, 88 Philip Street
Sydney NSW 2000
DX 117 Sydney
Ph: (02) 9921 8888   Fax: (02) 9921 8123
www.minterellison.com
Ref: CDSA

© CEC & NCISA 2001 1

NEALS
FOREWORD

The purpose of the Manual is to provide assistance and guidance to non-government schools in relation to the new requirements they must observe in relation to the preservation of an individual's privacy.

This Manual has been funded by the Association of Independent Schools and Catholic Education Commissions in each Australian State and Territory.

These requirements are new in Australia and are as yet untested. It is likely that over time experience will dictate that some change will need to be made to the procedures and forms suggested in the Manual. It is inevitable that some will place different interpretations on the requirements that schools need to fulfil.

In 2001, the Manual was shown to the then Privacy Commissioner, and his officers made some very helpful suggestions. The Privacy Commissioner does not endorse Manuals and has made it clear that complaints will be considered in particular circumstances in the context of their own merits. However, he welcomed the initiative of the Catholic Education Commission and National Council of Independent Schools' Associations in preparing this Manual to assist Schools in the area of privacy.

A significant part of the Privacy Commissioner's Guidelines are reproduced in the Manual with the permission of the Commissioner. However, we note that not all of the examples used in the Guidelines will be relevant to Schools. Also, we have made some minor alterations in our references to the Guidelines which do not alter their meaning or application.

As changes are made to the Manual, the 'Operative Data' contained on the cover sheet will be changed to indicate when the Manual was last revised. This should be checked on the relevant website at regular intervals.

DISCLAIMER

This Manual is for guidance only. Individual Schools and systems may wish to seek specific advice on how to comply with the Privacy Act.
TABLE OF CONTENTS

PART 1

1. INTRODUCTION .................................................................................................................. 7
   1.1 Purpose ............................................................................................................................ 7
   1.2 Background - the Privacy Act 1988 until 21 December 2001 ...................................... 7
   1.3 The Privacy Act 1988 from 21 December 2001 .............................................................. 7
   1.4 Health Records ............................................................................................................. 7
   1.5 National Privacy Principles .......................................................................................... 7
   1.6 Other Aspects of the Privacy Act .................................................................................. 7
   1.7 To whom will the Privacy Act apply? .......................................................................... 8
   1.8 Guidelines .................................................................................................................... 8
   1.9 Important Issues ......................................................................................................... 8

2. WHAT TYPES OF INFORMATION ARE COVERED BY THE ACT? ...................... 9
   2.1 The following types of information are covered by the Privacy Act: ............................ 9
   2.2 What is ‘personal information’? .................................................................................... 9
   2.3 What is ‘sensitive information’? ................................................................................... 9
   2.4 What is ‘health information’? ...................................................................................... 9
   2.5 What is a ‘record’? ....................................................................................................... 9
   2.6 Which acts and practices are exempt? ......................................................................... 10

3. COMPLIANCE: WHEN WILL THE ACT APPLY? ................................................. 12
   3.1 Information collected BEFORE AND AFTER commencement of the Act ............. 12
   3.2 Information collected AFTER commencement of the Act ........................................ 12
   3.3 Information Sheet 10 - Application of NPPs ............................................................. 12
   3.4 Application .................................................................................................................. 13

4. WHAT KINDS OF INFORMATION ARE COLLECTED AND HELD BY SCHOOLS? 14
   4.1 Personal information likely to be collected ................................................................. 14
   4.2 Sensitive information likely to be collected ............................................................... 14
   4.3 Health information likely to be collected .................................................................... 14

5. WHAT SCHOOLS NEED TO DO TO COMPLY ....................................................... 16
   5.1 Adoption of a Privacy Policy ...................................................................................... 16
   5.2 Appointment of a person/s responsible for privacy issues .......................................... 16
   5.3 Revision of current information handling practices and amendment of all relevant documentation and forms ................................................................................. 16
   5.4 Education of all staff and personnel ........................................................................... 17
   5.5 Provision of access to records ................................................................................... 17
   5.6 Complaints handling procedure and Breach of NPPs ................................................ 17
   5.7 Action Plan ................................................................................................................. 18

6. OBLIGATIONS IMPOSED BY THE NPPS: A BRIEF SUMMARY ....................... 20

7. COLLECTION (NPP 1 AND NPP 10) ................................................................. 22
   7.1 Collection (NPP 1) ..................................................................................................... 22
   7.2 What the Guidelines say: ......................................................................................... 22
   7.3 How to comply: ......................................................................................................... 22
   7.4 Lawful and fair collection (NPP 1.2) .......................................................................... 22
   7.5 What the Guidelines say: ......................................................................................... 22
   7.6 How to comply: ......................................................................................................... 23
   7.7 Ensuring the individual is fully aware of collection (NPP 1.3) .................................. 23
   7.8 What the Guidelines say: ......................................................................................... 23
   7.9 How to comply: ......................................................................................................... 24
   7.10 Standard Collection Notice .................................................................................... 22
   7.11 Verbal Collection .................................................................................................... 26
18.9 Access and Accuracy ........................................................................................................ 84
18.10 Disclosure and Use ........................................................................................................ 84
18.11 Schools as 'Health Service Provider' ............................................................................ 84
19. ANNEXURE A - PRIVACY POLICY .................................................................................. 86
19.1 A Privacy Policy is needed to inform individuals about the practices of the School in relation to personal information. It also serves as a guide to the School's staff as to the standards to be applied in respect of handling personal information and ensure consistency in the School's approach to privacy ............................................................ 86
20. ANNEXURE B - EMAIL AND INTERNET POLICY .......................................................... 96
20.1 Personal information may be collected, used, disclosed, stored and transferred overseas through the use of email and Internet facilities................................................................. 96
21. ANNEXURE C - NATIONAL PRIVACY PRINCIPLES ................................................... 102
21.1 Annexure C is the full text of the NPPs as contained in Schedule 3 to the Privacy Act. The NPPs and the Privacy Act are contained on the Privacy Commissioner's website: http://www.privacy.gov.au/publications/npps01.html#a ........................................ 102
22. ANNEXURE D - HEALTH PRIVACY PRINCIPLES - NEW SOUTH WALES ........ 113
23. ANNEXURE E - HEALTH PRIVACY PRINCIPLES - VICTORIA ................................ 128
24. ANNEXURE F - HEALTH PRIVACY PRINCIPLES - AUSTRALIAN CAPITAL TERRITORY ................................................................. 143
PART 1

1. INTRODUCTION

1.1 Purpose

1.1.1 The purpose of the Manual is to assist non-government schools and systems ('Schools') to implement the new Commonwealth privacy laws that come into effect on 21 December 2001.

1.1.2 The Manual describes the steps that need to be considered and changes that need to be considered to the existing policies of the Schools to ensure compliance with the new laws.

1.1.3 Through the Manual we have used the term 'Parents' to include parents or guardians.

1.2 Background - the Privacy Act 1988 until 21 December 2001

1.2.1 The Privacy Act 1988 is a Commonwealth Act that regulates the collection, storage, use and disclosure of different types of personal information by:

- Commonwealth and Australian Capital Territory government agencies
- credit providers
- credit reporting agencies, and
- organisations that use tax file numbers.

1.3 The Privacy Act 1988 from 21 December 2001

1.3.1 The Privacy Amendment (Private Sector) Act 2000 amends the Privacy Act 1988, so as to also regulate the way private sector organisations, including non-government schools and systems, handle 'personal information' of individuals. These amendments come into effect on 21 December 2001. In this Manual the original Act and the amendments are referred to as the 'Privacy Act'.

1.3.2 The purpose of the new provisions is to ensure that organisations that hold information about people handle that information responsibly. They aim as far as possible to establish a nationally consistent approach to the handling of personal information. The Privacy Act will govern how the School must handle personal information.

1.4 Health Records

1.4.1 Specific legislation was introduced in various states and territories which imposes certain limitations on how an organisation may deal with health records.

1.4.2 This legislation applies in New South Wales, Victoria and the Australian Capital Territory.

1.4.3 The obligations which apply in respect of health records are set out in Part 4.

1.5 National Privacy Principles

1.5.1 A key component of the legislation is the mandatory requirement for organisations to comply with the National Privacy Principles ('NPPs'). The NPPs set minimum standards which relate to the collection, security, storage, use, access, correction and disclosure of personal information. The NPPs are:

- briefly summarised in Section 6
- summarised individually in shaded boxes throughout this Manual, and
- set out in full at Annexure C in Section 21.
1.6 Other Aspects of the Privacy Act

1.6.1 The Privacy Act introduces a mechanism enabling individuals to:
(a) access personal information held about them
(b) request corrections be made to that information
(c) make complaints about the handling of their personal information, and
(d) receive compensation for interferences with their privacy.

1.6.2 The School will need to comply with the NPPs, or it may be liable to damages or required to comply with directions issued by the Privacy Commissioner.

1.6.3 In addition to its obligations under law, the School should remain alert to the Privacy Commissioner’s powers to publicise breaches of the Privacy Act in the media.

1.7 To whom will the Privacy Act apply?

1.7.1 The Act will apply to all ‘organisations’ in the private sector. An organisation includes:
(a) an individual
(b) a body corporate
(c) a partnership
(d) any other unincorporated association, or
(e) a trust.

1.7.2 There are some exemptions to the Privacy Act. These are discussed in paragraph 2.6 and Section 17.

1.8 Guidelines

1.8.1 The Privacy Commissioner has the power to make guidelines about the NPPs under the Privacy Act. The Guidelines are intended to provide advice and interpretation on how the NPPs will operate. The Guidelines are not binding. These have been incorporated in this Manual wherever relevant.

1.9 Important Issues

1.9.1 The Privacy Act does not differentiate between adults and children. Therefore, difficult issues arise about consents obtained from Parents for and on behalf of their children. When referring to consents and authorities throughout this Manual this should be borne in mind. The issue of consents and young people is discussed in paragraph 16.1.

1.9.2 If the School is a ‘credit provider’ it must also take into account provisions of the Privacy Act not affected by the amendments.
2. WHAT TYPES OF INFORMATION ARE COVERED BY THE ACT?

2.1 The following types of information are covered by the Privacy Act:
- personal information
- sensitive information, and
- health information.

2.2 What is ‘personal information’?

2.2.1 Personal information means information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It includes all personal information regardless of its source.

2.2.2 To put it more simply, it is information or an opinion that allows someone to identify the individual that the information or opinion is about. It can range from very detailed information such as medical records to other less obvious types of identifying information, such as an email address.

2.2.3 The NPPs apply to the collection of personal information by an organisation for inclusion in a record or a generally available publication, but apart from this, the NPPs only apply to personal information an organisation has collected that it holds in a record.

2.3 What is ‘sensitive information’?

2.3.1 Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record. It also includes health information.

2.4 What is ‘health information’?

2.4.1 Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual’s expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service. For more detail on the regulation of health information, see Part 4.

2.5 What is a 'record'?

2.5.1 The Privacy Act regulates personal information contained in a 'record'. A 'record' is defined as a document, database (however kept) or a photograph or other pictorial representation.

2.5.2 'Document' is not defined in the Act and a question arises as to whether a voice mail or sound recording would be classified as a 'record' under the Act. The School should treat voice mails and other sound recordings as being subject to the Privacy Act.

2.5.3 There are some items which are excluded from the definition of 'record'. The exclusions relevant to the School are:
(a) a generally available publication (eg a telephone directory), and
(b) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
2.5.4 The effect of these exclusions are discussed in paragraphs 16.8 and 16.9.

2.6 Which acts and practices are exempt?

2.6.1 The Privacy Act does exempt certain acts and practices by organisations. If acts and practices fall within one of the following categories, they are exempt from the scope of the Privacy Act.

2.6.2 The following is a summary only of some key exemptions that may be of relevance to the School:

### Small Business

2.6.3 A School with an annual turnover of $3 million or less will be deemed to be a 'small business' and will, subject to any exceptions, be exempt from the operation of the Privacy Act. The main exception relevant to Schools is where the School both holds health information (other than in an employee record) and provides a health service. In such a case, the School will not be considered a 'small business'.

2.6.4 Although the Act defines 'health service' broadly, this exception will mainly apply to Schools that have an infirmary or a registered nurse on staff who provides health services. It is likely, however, that most Schools that provide a 'health service' will have an annual turnover of greater than $3 million.

### Employee records

2.6.5 Certain acts or practices directly relating to employee records are exempt from the scope of the Act. Employee records are records relating to the employment of an employee of the employer. Examples of this type of information include the terms and conditions of employment, personal contact details, performance and conduct, disciplining, salary, termination and trade union membership.

2.6.6 This exemption only extends to current and previous employment relationships. It does not extend to prospective employees, nor to contractors and consultants. See paragraph 17.1.

2.6.7 In New South Wales there is an exemption in relation to health records of an employee. See Part 4.
Transfers between related companies

2.6.8 A related company or 'related body corporate' is as defined under the Corporations Act. Essentially, a related company refers to businesses that have a shared controlling interest. There will not be many Schools that will be related bodies corporate to other Schools within the meaning of the Corporations Act. Particular issues arise in this regard for school systems which may be based on religious structures such as Dioceses and separately incorporated Orders. These which are discussed separately.

2.6.9 In many circumstances Foundations and Trusts which are separately incorporated and established by a School are likely to be related bodies corporate of the School.

2.6.10 Under the Privacy Act, a company that is related to another company will be able to share and transfer personal information (but not sensitive information). However, those related companies must still comply with the NPPs in relation to the shared personal information.

2.6.11 The primary purpose of collection of the personal information of one body corporate will be deemed to be the same as that of the related body corporate which receives the information.

2.6.12 Note, therefore, that the information may not be used for any other purpose, other than that same primary purpose for which the information was collected by the original body corporate.

2.6.13 The related bodies corporate exemption applies only to the sharing of personal information (not sensitive information). Therefore, given that a large part of information that Schools collect and use is sensitive information (such as health information and religious information), this exemption may be of reduced significance. See paragraph 17.2.
3. COMPLIANCE: WHEN WILL THE ACT APPLY?

3.1 Information collected BEFORE AND AFTER commencement of the Act

3.1.1 The requirements of the NPPs that relate to:

(a) data quality - as it relates to use and disclosure (part of NPP 3)
(b) data security (NPP 4)
(c) openness (NPP 5)
(d) identifiers (NPP 7), and
(e) the transfer of personal information to another country (NPP 9),
will apply to personal information held by the School regardless of whether it was collected before or after the commencement of the Act.

3.1.2 NPP 6 (access & correction) applies to personal information collected after the commencement of the Act. However, NPP 6 will also apply to personal information collected before the commencement of the Act if the information is used or disclosed by the School after commencement, and where access or correction to the information will not cause an unreasonable administrative burden or expense.

3.2 Information collected AFTER commencement of the Act

3.2.1 The requirements of the NPPs that relate to:

(a) collection (NPPs 1 and 10) (and part of NPP 3 as it relates to collection)
(b) use and disclosure (NPP 2), and
(c) anonymity (NPP 8),
will only apply in relation to the collection of personal information after the commencement of the Act.

3.2.2 Therefore, subject to paragraph 3.1.2, where personal information is contained in a School's existing database, it will not be subject to the NPPs in this regard unless the information is subsequently updated.

3.2.3 In practical terms, it may become difficult for a School to identify which information is and is not subject to the Act. Further, Schools may not currently have the resources or systems to classify information on a database as 'subject to' or 'not subject to' the Act.

3.3 Information Sheet 10 - Application of NPPs

The following table (Table 1) is extracted from Information Sheet 10 which was recently released by the Privacy Commissioner. The table illustrates how the NPPs will apply to information which is held before, and information which is collected after, the commencement of the Privacy Act. Certain aspects of the Table which are of little relevance to Schools have been excluded.
Table 1

<table>
<thead>
<tr>
<th>NPP</th>
<th>Topic</th>
<th>What Information the NPP applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPP 1</td>
<td>Collection</td>
<td>only applies to information collected after 21 December 2001</td>
</tr>
<tr>
<td>NPP 2</td>
<td>Use and disclosure</td>
<td>only applies to information collected after 21 December 2001</td>
</tr>
<tr>
<td>NPP 3</td>
<td>Data quality and collection</td>
<td>as it applies to collection only applies to information collected after 21 December 2001</td>
</tr>
<tr>
<td>NPP 3</td>
<td>Data quality on use and disclosure</td>
<td>as it applies to use and disclosure it applies regardless of when it was collected.</td>
</tr>
<tr>
<td>NPP 4</td>
<td>Data security</td>
<td>applies regardless of when information was collected</td>
</tr>
<tr>
<td>NPP 5</td>
<td>Privacy policies and openness</td>
<td>applies regardless of when information was collected</td>
</tr>
<tr>
<td>NPP 6</td>
<td>Access and correction</td>
<td>if information already held is not used or disclosed it only applies to information collected after 21 December 2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>But</td>
</tr>
<tr>
<td></td>
<td></td>
<td>if information already held is used or disclosed after commencement then rights of access and correction apply unless</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• unreasonable administrative burden or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cause the organisation unreasonable expense.</td>
</tr>
<tr>
<td>NPP 7</td>
<td>Commonwealth Government identifiers</td>
<td>applies regardless of when information collected</td>
</tr>
<tr>
<td>NPP 8</td>
<td>Anonymity</td>
<td>only applies to information collected after 21 December 2001</td>
</tr>
<tr>
<td>NPP 9</td>
<td>Transborder data flow</td>
<td>applies regardless of when information collected</td>
</tr>
<tr>
<td>NPP 10</td>
<td>Collection of sensitive information</td>
<td>only applies to information collected after 21 December 2001</td>
</tr>
</tbody>
</table>

3.4 Application

3.4.1 Schools may need to take into account particular practices and laws that exist in the State or Territory in which they operate. It is not thought that there are many (if any) circumstances which are different and the great majority of recommendations will be appropriate to all non-government schools and systems.
4. WHAT KINDS OF INFORMATION ARE COLLECTED AND HELD BY SCHOOLS?

4.1 Personal information likely to be collected

4.1.1 The following kinds of personal information are likely to be collected and held in a 'record' (which is defined by the Act to be a document, database or photograph).

4.1.2 For pupils this could include:
- name, address, phone number, date of birth (and age), birth certificate, conduct reports, next of kin details, emergency contact numbers, names of doctors, school reports, assessments, referrals (eg government welfare agencies/departments), correspondence with parents, photos, current/previous school, health fund details and Medicare number.

4.1.3 For parents this could include:
- name, address, email address, phone number, date of birth, vehicle registration details, occupation, marital status/problems, custody details, doctor’s name and contact information, Medicare number, other children’s details, donation history, maiden name of ex-pupils, alumni year, whether alumni had further education, professional experience, personal news.

4.1.4 For job applicants, staff members and contractors this could include:
- name, company name and ABN, phone number, email address, TFN, date of birth and age, contact details of next of kin, emergency contact numbers, including doctor, residency status/work visa status, qualifications, education, academic transcript, work permit, Passport, details of previous salary, salary being sought and other salary details, details of referees, bank account number, superannuation details, marital status, letters of appointment/complaint/ warning/resignation, record of interview, leave applications, discipline issues, professional development appraisals, performance review, photograph, applications for promotions, references, commencement date, employment agency details and former employers.

4.1.5 Personal information might also be collected from other people such as board members, committee members, volunteers, neighbours, donors and others.

4.2 Sensitive information likely to be collected

4.2.1 The following kinds of sensitive information are likely to be collected and held by Schools.

4.2.2 For pupils:
- religion, birth certificate, language spoken at home, religious records, whether Aboriginal, nationality, country of birth, Sacrament/Parish (current Parish, name of referring Priest, date and place of Baptism, Confirmation, Eucharist and Reconciliation), and Baptism Certificate.

4.2.3 For parents:
- religion, country of birth and nationality

4.2.4 For job applicants, staff members and contractors:
- place of birth, religion, religious education, criminal record check, relevant child protection law information, member of professional associations, trade union membership, country of birth and nationality.

4.3 Health information likely to be collected

4.3.1 The following types of health information are likely to be collected and held by Schools.

4.3.2 For pupils:
- medical background, immunisation records, medical records, medical treatments, accident reports, absentee notes, medical certificates, height and weight, nutrition and dietary
requirements, assessment results for vision, hearing and speech, reports of physical
disabilities, illnesses, operations, paediatric medical, psychological, psychiatric and
psychometric information, developmental history, diagnosis of disorders, learning details
(recipient of special procedures, assessment for speech, occupational, hearing, sight, ADD,
Educational Cognitive (IQ)).

4.3.3 For parents:
history of genetic and familial disorders (including learning disabilities), miscellaneous
sensitive information contained in a doctor or hospital report.

4.3.4 For job applicants, staff members and contractors:
medical condition affecting ability to perform work, health information, compensation
claims and doctor’s certificates.
5. WHAT SCHOOLS NEED TO DO TO COMPLY

5.1 Adoption of a Privacy Policy

5.1.1 The School will be required to adopt a Privacy Policy which expresses, in plain language, the School’s policy or policies on its management of personal information.

5.1.2 A draft Privacy Policy is attached in Appendix B (see Section 19) which can be adapted as required by the relevant School to accurately reflect the acts and practices of the Schools who adopt it (that is, all relevant Schools who are subject to the Privacy Act). This can be used to help inform individuals about the practices of the School in relation to personal information. It would also serve as a guide to the School’s staff as to the standard to be applied in handling personal information and ensure consistency in the School’s approach to information privacy.

5.1.3 The draft Privacy Policy provides a template for setting out:

(a) the School’s commitment to the NPPs
(b) the types of information that will be collected, used and disclosed, and the purpose for which it is collected;
(c) the management and use of the information collected, and in particular sensitive health information; and
(d) management of issues relating to access and correction.

5.1.4 The School should amend the template to reflect accurately its own particular acts and practices.

5.2 Appointment of a person/s responsible for privacy issues

5.2.1 The School's administering body will need to examine what information it collects and how it deals with it. Although not required by the Act, the School should consider nominating a person responsible for privacy (the privacy contact). This person should be a senior current staff member. The person appointed should be familiar with the School's Privacy Policy.

5.2.2 The School may prefer the privacy contact to be the Principal.

5.3 Revision of current information handling practices and amendment of all relevant documentation and forms.

5.3.1 Only information which is necessary to fulfil the School’s functions and activities should be collected. The School should determine what information they collect, revise forms to reflect the Privacy Policy, provide information about collection and, where necessary, obtain consents to the collection, use and disclosure of that information.

5.3.2 At or soon after the time of collection the School must take reasonable steps to notify the individual of the following:

(a) its identity and contact details
(b) the purpose of collection
(c) the individual’s right to access the information
(d) the types of organisations to which it usually discloses the information
(e) laws that require collection, and
(f) the consequences of not providing the information.

5.3.3 The School should include in enrolment and job application forms a 'standard collection notice' (see paragraph 7.10). All existing parents and staff members should be provided with a 'standard collection notice'.
5.4 Education of all staff and personnel

5.4.1 This would include:

(a) distribution of the School’s Privacy Policy to all current staff and relevant personnel
(b) acknowledgment by all existing staff and relevant personnel that they have read and understood the Privacy Policy
(c) incorporation of the Privacy Policy into the terms and conditions of employment or engagement for all new staff and contractors, and acknowledgment that they have read and understood it
(d) appropriate reminders and notifications throughout the School of commitment to the NPPs, and
(e) periodic compliance reviews and audits.

5.5 Provision of access to records

5.5.1 The School should have, where possible, standard policies in relation to access to, and correction of, records which contain personal information. The ‘access’ requirements will apply in three sets of circumstances:

(a) pupils, Parents and others seeking access to their personal information
(b) contractors, prospective employees and unsuccessful job applicants seeking access to their personal information
(c) employees seeking access to their records where those records do not relate to an act or practice directly related to employment relationship (eg in their role as a Parent of a pupil at the School).

5.5.2 Where there is a disagreement about the accuracy, completeness or currency of the personal information, and the individual asks the School to attach a statement claiming that the information is not accurate, complete or current, then the School must take reasonable steps to do so.

5.5.3 Personal information directly relating to an 'employee record' is exempt from the Privacy Act. Therefore employees of the School (whose records are exempt from the Act) may be refused access to, and the ability to correct, their personal information held by their employer. This exemption is discussed in more detail in paragraph 17.

5.6 Complaints handling procedure and Breach of NPPs

5.6.1 The Act enables individuals to make a complaint if they feel their personal information has been handled inappropriately by the School.

5.6.2 Complaints need to be directed in the first instance to the School.

5.6.3 The Privacy Commissioner may not investigate a matter if the individual has not first brought a complaint to the School concerned, unless the Privacy Commissioner is of the view that this would be inappropriate.

5.6.4 For this reason, the School may wish to develop, in conjunction with its Privacy Policy, a complaints handling procedure.

5.6.5 If the complaint is unable to be resolved at the School level, the Privacy Commissioner may investigate the complaint. A complaint that is upheld may be resolved by an order that the organisation redress any loss or damage to the person whose privacy has been breached. This could include a compensation order.

5.6.6 Notwithstanding the procedures described above, the Privacy Commissioner also has discretion to investigate, on his own initiative, an act or practice which may be an interference with privacy if the Privacy Commissioner thinks that it would be appropriate...
(eg, even where no complaint has been made by the individual involved).

5.6.7 If the organisation does not comply with any orders made, the complainant can have the order enforced in the Federal Court or the Federal Magistrates Court.

5.6.8 The Privacy Commissioner has indicated that the complaints process is designed to ensure that most complaints can be resolved through conciliation and mediation rather than through the courts.

5.7 Action Plan

5.7.1 The School should consider using the following action plan in taking steps to comply with the Privacy Act:

**Internal Review**
- consider appointing privacy contact person
- conduct a review of current information handling practices

**Results of Review**

Analyse results of the review to identify:
- what information the School collects about whom and from whom
- why and how the School collects, uses and discloses personal information
- any risk areas (e.g. where there is collection and use of sensitive information or where collection, use or disclosure of personal information might not be expected by the individual), and
- what changes need to be made

**Privacy Policy**
- formalise and implement a Privacy Policy (this may be adapted from a relevant policy in Section 19)

**Before 21 December 2001**
- put in place systems and procedures for information collected before 21 December 2001 (eg discard information no longer needed, establish systems to make data secure)

**After 21 December 2001**
- put in place systems and procedures for information collected after 21 December 2001 (eg put in place collection notices, amend employment contracts, put in place process to allow access to records, establish systems to make data secure, educate employees)
- consider whether a complaints handling procedure should be drafted

**Continuing Obligations**
- make Privacy Policy available to anyone who asks for it
- ensure on-going compliance (eg regular review of information handling practices, conduct further audits where necessary, update Privacy Policy and collection notices)
• ensure compliance with other applicable health records legislation (see Part 4).
6. OBLIGATIONS IMPOSED BY THE NPPS: A BRIEF SUMMARY

6.1.1 This is a summary only and NOT a full statement of obligations. These are set out in the NPPs. The summary was prepared by the Office of the Federal Privacy Commissioner. A full version of the NPPs is contained in Annexure C in Section 21.

- Only collect personal information that is necessary for your functions or activities.
- Use fair and lawful ways to collect personal information.
- Collect personal information directly from an individual if it is reasonable and practicable to do so.
- Get consent to collect sensitive information unless specified exemptions apply.
- At the time you collect personal information or as soon as practicable afterwards, take reasonable steps to make an individual aware of:
  - why you are collecting information about them;
  - who else you might give it to; and
  - other specified matters.
- Take reasonable steps to ensure the individual is aware of this information even if you have collected it from someone else.
- Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in NPP 2.1 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances). Note that:
  - If the information is sensitive the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related and the direct marketing provisions of NPP 2.1(c) do not apply.
- Take reasonable steps to ensure the personal information you collect, use or disclose is accurate, complete and up-to-date. This may require you to correct the information.
- Take reasonable steps to protect the personal information you hold from misuse and loss and from unauthorised access, modification or disclosure.
- Take reasonable steps to destroy or permanently de-identify personal information if you no longer need it for any purpose for which you may use or disclose the information.
- Have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it.
- If an individual asks, take reasonable steps to let them know, generally, what sort of personal information you hold, what purposes you hold it for and how you collect, use and disclose that information.
- If an individual asks, you must give access to the personal information you hold about them unless particular circumstances apply that allow you to limit the extent
to which you give access - these include emergency situations, specified business imperatives and law enforcement or other public interests.

- Only adopt, use or disclose a Commonwealth Government identifier if particular circumstances apply that would allow you to do so.
- If it is lawful and practicable to do so, give people the option of interacting anonymously with you.
- Only transfer personal information overseas if you have checked that you meet the requirements of NPP 9.
PART 2 - NATIONAL PRIVACY PRINCIPLES

7. COLLECTION (NPP 1 AND NPP 10)

7.1 Collection (NPP 1)

7.1.1 Requirement:
An organisation must not collect personal information unless necessary for one or more of its functions or activities. (NPP 1.1)

7.2 What the Guidelines say:

7.2.1 The Commissioner interprets 'necessary' in a practical sense. If an organisation cannot effectively pursue a legitimate function or activity without collecting personal information, then ordinarily such collection would be deemed to be 'necessary' for one or more of its functions or activities. An organisation should not collect information on the 'off-chance' that it will be of some use in the future.

7.2.2 The collection of personal information which is required by law would be deemed as being 'necessary' for one or more of an organisation's functions or activities.

7.3 How to comply:

7.3.1 Review Section 4 to ensure that all items of personal information collected by the School have been identified.

7.3.2 Ensure that all items of personal information identified are reviewed as to whether their collection is necessary for one or more of the School's functions or activities.

7.3.3 If new items of personal information are proposed to be collected in the future from individuals or from third parties (eg through the anticipated increasing use of the Internet), and whether as part of existing or new activities, then those items should be subject to scrutiny as to the necessity of collecting the information.

7.3.4 The School must carefully consider whether the personal information it collects is necessary for one or more of its functions or activities.

7.4 Lawful and fair collection (NPP 1.2)

7.4.1 Requirement: An organisation must collect personal information:
(a) only by lawful and fair means, and
(b) not in an unreasonably intrusive way.

7.5 What the Guidelines say:

Generally, 'fair' means without intimidation or deception. For example, usually covert collection will be considered as unfair collection.

7.5.1 Examples of what might be considered unfair or unreasonably intrusive ways of collection include:
(a) calling an individual late at night or at meal time without a prior arrangement to do so
(b) asking for information for one purpose when really it is for another purpose,
(c) telling an individual that it is compulsory that they provide personal information when it is not, and
(d) asking for sensitive personal details within earshot of other people.

7.6 How to comply:

7.6.1 The School should regularly review its collection procedures and particular acts and practices of collection should be identified and monitored for instances (whether systemic or by particular individuals) of unfair collections or unreasonably intrusive collections.

7.6.2 Any complaints concerning the methods of collection should be part of this monitoring process.

7.6.3 The School should be careful to consider and re-consider the context in which personal information is collected and should always be mindful that personal information and sensitive information should be collected discreetly where possible.

7.7 Ensuring the individual is fully aware of collection (NPP 1.3)

<table>
<thead>
<tr>
<th>Requirements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>At or before the time (or, if not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to make the individual aware of:</td>
</tr>
</tbody>
</table>

| (a) | the organisation's identity and contact details |
| (b) | the individual's access rights to the information |
| (c) | why the information is being collected |
| (d) | to whom the information is usually disclosed |
| (e) | any law that requires the collection of the information, and |
| (f) | the main consequences, if any, of the individual not providing the information. |

7.8 What the Guidelines say:

7.8.1 Meaning of 'at or before time of collection'

Deciding on whether an organisation can make individuals aware of at or before the time of collection will depend on the circumstances. This could be done after collection if there are practical problems in doing so before collection.

7.8.2 Meaning of 'reasonable steps'

Where the circumstances of collection make a matter listed in NPP 1.3 obvious, then the 'reasonable steps' might not involve any active measures because the circumstances speak for themselves. For example, if the matters contained in NPP 1.3 were made available to an individual for a certain type of collection, then the same collection later may not require that the NPP 1.3 matters (if unchanged) be repeated to the individual. Deciding what are reasonable steps involves balancing a number of possible factors, including the importance to the individual of having the relevant knowledge and the cost to the organisation in providing that information.
7.8.3 Meaning of NPP 1.3(c)

The description of the purposes can be reasonably general as long as the description is adequate to ensure that the individual is aware of what is going to be done with their personal information. Internal purposes that form part of normal business practices, such as auditing, business planning or billing do not have to be described.

7.8.4 Meaning of NPP 1.3(d)

‘Reasonable steps’ to inform an individual about usual disclosures would ordinarily mean either giving general descriptions of sets of people and organisations (for example, ‘State Government licensing authorities’, ‘health insurers’ and ‘list renters’) or to list each member of the set.

An organisation does not need to mention disclosures that the NPPs permit, but in practice happen only rarely. For example, it does not need to mention disclosures under warrant or to intelligence agencies.

7.8.5 Meaning of NPP 1.3(e)

Reasonable steps must be taken to tell the individual about any law that requires the individual to provide, or the organisation to collect, personal information in the particular situation. In describing the law the organisation need not specify the exact piece of legislation (although it would be desirable to do this where possible). A statement like ‘Taxation law requires us to collect this’ would ordinarily be adequate.

7.8.6 Meaning of NPP 1.3(f)

An organisation need not describe all possible consequences of not providing personal information. Ordinarily significant (and non-obvious) consequences would need to be described. Often this would mean that the organisation makes clear which items are essential to fulfil the primary purpose of collection. An example of such a statement might be ‘if you don’t tell us this, we won’t be able to process your application’.

7.9 How to comply:

7.9.1 A common sense and pragmatic approach should be taken by the School when complying with NPP 1.3.

7.9.2 In many cases, a 'standard collection notice' (which would operate throughout the time the child is enrolled at the School) (see paragraph 7.10.1) and an 'employment collection notice' (see paragraph 7.13) would cover most situations of collection of personal information by the School and would be compliant with NPP 1.3.

7.9.3 However, where the School collects personal and sensitive information from those who have not seen either collection notices (eg third parties) or where the collection notices do not cover a particular situation, then the School should consider, with reference to the NPPs and Guidelines, at to whether it needs to take additional steps to comply with NPP 1.3.

7.9.4 The 'standard collection notice', which is drafted to cover the School's usual collection practices, could be tailored to suit specific situations and should deal with the matters listed in NPP 1.3 concerning how any personal and sensitive information collected from the individual about him/herself or a third party would be dealt with.

7.9.5 The 'standard collection notice' would be reproduced in enrolment forms, be contained in the School's Privacy Policy and should be located on the School's website (where applicable). All current Parents should be sent a copy of the 'standard collection notice'.

7.9.6 The School should consider placing a 'standard collection notice' in other relevant documents.
The 'standard collection notice' should be distributed with all enrolment forms to pupils' Parents. It could also be placed in each pupil's School diary. It is suggested that the notice be sent each year to Parent's of pupils at the same time as other materials are sent. It should be updated annually.

7.10 7.10 Standard Collection Notice (Revised 28/11/11)

The following is suggested wording which seeks to achieve a combination of ensuring the individual is reasonably aware of the matters specified in NPP 1.3 and also to obtain consent for uses and disclosures of personal information that may not be regarded as being for primary or secondary related (or directly related) purposes to the collection:

1. The School (the Diocese both independently and through its Schools) collects personal information, including sensitive information about pupils and parents or guardians before and during the course of a pupil's enrolment at the School. The primary purpose of collecting this information is to enable the School to provide schooling for your son/daughter.

2. Some of the information we collect is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.

3. Certain laws governing or relating to the operation of schools require that certain information is collected. These include Public Health [and Child Protection]* laws.

4. Health information about pupils is sensitive information within the terms of the National Privacy Principles under the Privacy Act. We ask you to provide medical reports about pupils from time to time.

5. If we do not obtain the information referred to above we may not be able to enrol or continue the enrolment of your son/daughter.

6. The School from time to time discloses personal and sensitive information to others for administrative and educational purposes. This includes to other schools, government departments, government agencies, statutory boards [Catholic Education Office, the Catholic Education Commission, your local diocese and the parish, Schools within other Catholic Dioceses. Also government authorities such as the NSW Board of Studies, the Australian Curriculum, Assessment and Reporting Authority (ACARA)]* medical practitioners, and people providing services to the School, including specialist visiting teachers, [sports] coaches, volunteers and counsellors.

6a. In addition to the agencies and purposes cited at 6 above personal information relating to students and parents may also be made available, in accordance with Australian Government requirements, to ACARA for the purpose of publishing certain school information relating to the circumstances of parents and students on the MySchool website.

7. The School from time to time may also collect and disclose personal information about current or prospective students in accordance with the Education Act or child protection legislation.*

8. Personal information collected from pupils is regularly disclosed to their parents or guardians. On occasions, information such as academic and sporting achievements, pupil activities and other news is published in School newsletters, magazines [and on our website].

9. Parents may seek access to personal information collected about them and their son/daughter by contacting the School. Pupils may also seek access to personal information about them. However, there will be occasions when access is denied. Such occasions would include where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the School’s duty of care to the pupil, or where pupils have provided information in confidence.
10. As you may know the School from time to time engages in fundraising activities. Information received from you may be used to make an appeal to you. [It may also be disclosed to organisations that assist in the School's fundraising activities solely for that purpose.] We will not disclose your personal information to third parties for their own marketing purposes without your consent.

11. On occasions information such as academic and sporting achievements, pupil activities and similar news is published in School newsletters and magazines [and on our website]

[12. We may include your contact details in a class list and School directory]**

13. If you provide the School with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties.

14. The school may utilise service providers to provide certain services including data storage to the school and its staff and students. The school may provide your personal information to such service providers in connection with the provision of these services. The school’s email service provider may store and process emails outside Australia. The school’s service provider may also store data outside Australia.

* If appropriate
** Schools may wish to seek specific consent to publish contact details in class lists and School directories

7.11 Verbal Collection

7.11.1 Where records of personal information are made from telephone conversations, appropriate steps should be taken to make the individual aware of the matters contained in 'standard collection notice' unless they are otherwise aware of these matters or they are reasonable obvious. Such steps should also be taken in relation to the creation of records containing personal information as a result of face to face contact.

7.12 Alumni Collection Notice

7.12.1 At some Schools, pupils' personal information will be sent to the School's alumni or similar association when the pupil leaves the School. When this occurs the School should obtain the pupil's consent to this and should insert an appropriate collection notice in a relevant form (eg Application for membership of Alumni Association form). If the pupil is young, such as when leaving a preparatory school, it may be appropriate to seek the Parent's consent to include the child's name on an Alumni register.

7.12.2 Alternatively, the School might wish to forward to the pupil, on behalf of the Alumni association, relevant documentation inviting the pupil to join the association.
Such a collection notice could be worded as follows:

**Alumni Collection Notice**

1. [The Alumni Association/We] may collect personal information about you from time to time. The primary purpose of collecting this information is to enable us to inform you about our activities and the activities of [name of School] and to keep alumni members informed about other members.

2. We must have the information referred to above to enable us to continue your membership of [the Alumni Association].

3. As you know, from time to time we engage in fundraising activities. The information received from you may be used to make an appeal to you. [It may also be used by [name of School] to assist in its fundraising activities.] [If you do not agree to this, please advise us now]

4. [The Alumni Association/We] may publish details about you in our [name of publication] [and our/the School's website]. If you do not agree to this you must advise us now.

5. You may seek access to personal information collected about you by contacting [us, care of the School].

6. If you provide personal information to us about other people, we encourage you to inform them of the above matters.

**Employment Collection Notice**

7.13.1 When receiving employment applications an 'employment collection notice' should be sent to the individual with the acknowledgment. This notice could be worded as follows:

**Employment Collection Notice**

1. In applying for this position you will be providing [name of School] with personal information. We can be contacted [insert address, email address, telephone number].

2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application.

3. You may seek access to your personal information that we hold about you if you are unsuccessful for the position. However, there may be occasions when access is denied. Such occasions would include where access would have an unreasonable impact on the privacy of others.

4. We will not disclose this information to a third party without your consent. / We usually disclose this kind of information to the following types of organisations [insert list].

5. [We are required to [conduct a criminal record check] collect information [regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences] under Child Protection laws.*] We may also elect to collect personal information about you in accordance with these laws.*

6. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish, that the School does not usually disclose the information to third parties.* If applicable in the relevant state.
7.13.2 The employee records exemption (see paragraph 17) does not apply to job applicants. Therefore, under NPP 6 (see Section 12) job applicants may seek access to records of personal information which the School holds about them. The School should be mindful of this when collecting personal information (eg references, making notes and reports). The School might consider destroying some or all records once the position is filled. The same applies to contractors.

7.13.3 When collecting sensitive information, NPP 10 requires that consent be obtained, unless an exception applies (such as where collection is required by law - NPP 10.1(b)). Regardless of whether consent for collection is required, NPP 1 must still be complied with. This issue is discussed in paragraph 7.26.5.

7.13.4 If unsolicited job applications are received and the School wishes to retain the applicant's information, the 'employment collection notice' should be sent. However, if you

7.13.5 intend to pass on information to a related School, you should make the applicant aware of this in the 'employment collection notice'.

7.14 Contractor/Volunteer Collection Notice

7.14.1 All new contractors and volunteers should be sent a modified version of the 'employment collection notice'. Such an amended notice could be worded as follows:

**Contractor / Volunteer Collection Notice**

1. In applying to provide your services you will be providing [name of School] with personal information. We can be contacted [insert address, email address, telephone number].

2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.

3. You agree that we may store this information for [insert amount of time].

4. Access to this information may be available to you if you ask the School for it.

5. We will not disclose this information to a third party without your consent. / We usually disclose this kind of information to the following types of organisations [insert list].

6. [We are required to [conduct a criminal record check] collect information [regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences] under Child Protection law.*] [We may also elect to collect personal information about you in accordance with these laws.*]

7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties.

* If applicable in the relevant state.

7.15 Collection through monitoring of computer use

7.15.1 People using schools' computer systems, networks and facilities should be advised through a computer usage policy that their use will/may be monitored. If computer use is being monitored, personal information may be collected.
In NSW, specific legislation requires employers to notify their employees in advance that their use will be monitored.

Students, volunteers, teachers, employees and contractors should be provided with a computer usage policy. Ideally, written acknowledgement that they have received that policy should be given to the school.

An example policy for teachers, employees and contractors is at paragraph 20, Annexure B.

7.16 Collection of information directly (NPP 1.4)

7.16.1 Requirement:
If reasonable and practicable, personal information must only be collected directly from the individual.

7.17 What the Guidelines say:
NPP 1.4 aims to ensure that where it is reasonable and practicable to do so an organisation will collect information about an individual only from that individual.

7.17.1 In the case of Schools this is often not practicable.

7.17.2 Personal information is collected by Schools in a number of different ways. The following table indicates direct collections:

<table>
<thead>
<tr>
<th>Collection point</th>
<th>Collection method (&amp; source)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct contact</td>
<td>employment interviews (employees and job applicants)</td>
</tr>
<tr>
<td></td>
<td>meetings (eg P&amp;F) (from Parents)</td>
</tr>
<tr>
<td></td>
<td>face-to-face contact with pupils, staff members and Parents</td>
</tr>
<tr>
<td></td>
<td>writing (eg letters from Parents)</td>
</tr>
<tr>
<td>Forms and Documentation</td>
<td>enrolments forms (Parents)</td>
</tr>
<tr>
<td></td>
<td>medical forms (Parents)</td>
</tr>
<tr>
<td></td>
<td>various other forms concerning pupils, staff members and Parents</td>
</tr>
<tr>
<td></td>
<td>emails and Internet</td>
</tr>
<tr>
<td>Telephone</td>
<td>Calls received from:</td>
</tr>
<tr>
<td></td>
<td>Parents</td>
</tr>
<tr>
<td></td>
<td>staff members</td>
</tr>
<tr>
<td></td>
<td>others</td>
</tr>
</tbody>
</table>

7.17.3 There are also various methods of indirect collection, including interviews, forms and other documentation, telephone calls, references, and resumes.
The following indicates some instances of indirect collection by Schools:

<table>
<thead>
<tr>
<th>Individual concerned</th>
<th>Third party source of collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pupils of another school</td>
<td>Principal of another school</td>
</tr>
<tr>
<td>Pupils</td>
<td>Professionals (e.g. counsellors, doctors, speech pathologists, therapists, other agencies) through reports and general information (e.g. medical, vision, hearing, speech tests) and other results (e.g. psychometric)</td>
</tr>
<tr>
<td>Pupils</td>
<td>Parents and staff in performance appraisals</td>
</tr>
<tr>
<td>Pupils</td>
<td>CEC and AIS</td>
</tr>
<tr>
<td>Pupils</td>
<td>School (teachers, principal, boarding master) (e.g. where computer use is monitored, certain access to personal and disciplinary information)</td>
</tr>
<tr>
<td>Pupils</td>
<td>Parent through various forms (e.g. enrolment form, medical advice form, deed of indemnity)</td>
</tr>
<tr>
<td>Pupils</td>
<td>Government welfare agencies/departments (regarding safety of child at home)</td>
</tr>
<tr>
<td>Pupils</td>
<td>Parent (and vice versa)</td>
</tr>
<tr>
<td>Pupils and staff members</td>
<td>Pupils and/or staff members through various forms (e.g. incident report, Child Protection Notification Form)</td>
</tr>
<tr>
<td>Pupils, staff members, others</td>
<td>Pupils who name them to counsellors or staff members during counselling or advising or in an incident report</td>
</tr>
<tr>
<td>Pupils and Parents</td>
<td>Priests (reference)</td>
</tr>
<tr>
<td>Pupils or prospective pupils in NSW</td>
<td>Previous school (reference)</td>
</tr>
<tr>
<td>Pupils or prospective pupils in NSW</td>
<td>Another school for the purpose of assessing whether the enrolment of the pupil or prospective pupil would pose a risk to the health or safety of any person and to develop and maintain strategies to eliminate or minimise that risk*</td>
</tr>
<tr>
<td>Parents</td>
<td>Other Parents or others (e.g. P&amp;F, development office for fundraising)</td>
</tr>
<tr>
<td>Parents</td>
<td>Medical practitioners (e.g. mother has cancer)</td>
</tr>
<tr>
<td>Parents</td>
<td>School (e.g. in Pupil Report Card)</td>
</tr>
<tr>
<td>Pupils’ family members</td>
<td>Pupil (e.g. pray for sick Parent or Grandmother)</td>
</tr>
</tbody>
</table>

* The laws relating to this form of collection are not yet in force. Please refer to paragraph 16.7 of this Manual for more information.

<table>
<thead>
<tr>
<th>Individual concerned</th>
<th>Third party source of collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees and Contractors</td>
<td>Referees who provide information upon request</td>
</tr>
<tr>
<td>Previous employers</td>
<td>Staff members and job applicants through various forms (e.g. application form) and resume</td>
</tr>
<tr>
<td>Individual concerned</td>
<td>Third party source of collection</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Job applicants</td>
<td>• Previous employers</td>
</tr>
<tr>
<td></td>
<td>• Police through criminal record checks</td>
</tr>
<tr>
<td>Spouses of job applicants</td>
<td>• Job applicants through provision of marriage certificate. We presume this personal information is 'collected'.</td>
</tr>
<tr>
<td>Contractors</td>
<td>• Dun &amp; Bradstreet due diligence search</td>
</tr>
<tr>
<td>Referees</td>
<td>• Staff members and job applicants through various forms</td>
</tr>
<tr>
<td>Next of kin</td>
<td>• Pupils, staff members and Parents through various forms (eg enrolment form)</td>
</tr>
<tr>
<td>Emergency contacts</td>
<td>• Pupils, staff members and Parents through various forms (eg enrolment form, staff detail form)</td>
</tr>
<tr>
<td>Nominated siblings/family members</td>
<td>• Pupils and Parents through various forms (eg enrolment form)</td>
</tr>
<tr>
<td>Doctor</td>
<td>• Parent (eg from enrolment form, pupil information sheet)</td>
</tr>
<tr>
<td>Others</td>
<td>• photographs</td>
</tr>
</tbody>
</table>

7.17.6 It is apparent that it will not always be reasonable and practicable to collect personal information from the individual directly. In most scenarios, the individual concerned is aware of this indirect collection. However, this may not always be the case.

7.17.7 Where a job applicant is aware that a referee is providing information about them to a School (therefore indirect collection), it can be implied that they consent to that indirect collection. However, if the School collects personal information from a referee or third party without the applicant's knowledge (eg the job applicant's current employer), the School should obtain the individual's consent to collect the information. If applicants decline to give consent and this may prejudice their application, then NPP 1.3 requires that the they be informed of this.

7.17.8 NPP 1.4 (as with all other NPPs) will not apply to employee's personal information so long as the individual is an employee and the information is classified as an 'employee record' under the employee records exemption in the Privacy Act. This is discussed in more detail in Section 17.

'Reasonable steps' in the context of NPP 1.4 (and NPP 1.5) would depend on the circumstances. Some of the matters to be considered are:

(a) whether it is possible to collect the information directly
(b) whether a reasonable individual might expect information about them to be collected directly or indirectly
(c) how sensitive the information is
(d) the cost of collecting the information directly rather than indirectly
(e) the privacy consequences for the individual if the information is collected indirectly, and
(f) what is accepted practice (by consumers and the industry).

7.18 How to comply:

7.18.1 There may be some circumstances in which collection of information directly from the individual concerned should occur. These circumstances should be considered on a case by case basis.
Example:
Where it is likely that the information is incorrect (eg the source is unreliable) then the School collecting the information should endeavour to contact the individual concerned to check whether the information is accurate. It will not always be reasonable and practicable to do this. For example, the individual concerned may be the subject of an allegation about an unlawful activity and approaching that person may prejudice the investigation.

7.19 Ensuring the individual is fully aware of an indirect collection (NPP 1.5)

7.19.1 Requirement:
Where personal information is collected about an individual from someone else, the organisation must take reasonable steps to ensure that the individual is made aware of the matters listed in NPP 1.3.

7.20 What the Guidelines say:
The aim of NPP 1.5 is to ensure that an individual knows what happens to information about them regardless of whether the information is collected directly or indirectly.

If an organisation collects information from a generally available publication NPP 1.5 may not apply depending on the circumstances (see paragraph 16.8).

7.20.1 The steps the School may need to take to make an individual aware of the matters listed in NPP 1.3 when collecting their personal information indirectly will depend on the circumstances. Deciding what are 'reasonable steps' where the School collects personal information in such a case involves balancing factors of a similar kind to those for NPP 1.4 (see paragraph 7.16).

7.21 How to comply:
7.21.1 The School should consider, on a case by case basis, when collecting personal information indirectly, what, if any, (reasonable) steps the School should take to make the individual aware of the matters listed in NPP 1.3.

7.21.2 As indicated in paragraph 16.9.2, when collecting personal information for inclusion in a School publication, the School should collect personal information and sensitive information from the individual directly. This is particularly relevant where the information is of a personal or private nature (such as an illness, marriage or birth of a child) and where publication of the information (if incorrect or without consent) might result in embarrassment or other adverse consequences to the individual. On the other hand, collection of information as to an individual's job appointment which is public knowledge (such as an appointment to UNICEF) is unlikely to cause difficulty.

7.21.3 These comments should be considered in the context of an alumni receiving an 'alumni collection notice' (see paragraph 7.12.3) which states that their information may be published by the association. It should be remembered that the 'alumni collection notice' will only act as a notice to alumni and not to third parties (such as children or spouses).
7.22 Collection, use and disclosure with third parties and contractors (NPP 1.5 and NPP 2)

7.22.1 Where the School engages a contractor or third party the following may occur:

(a) the School collects personal information from a contractor or third party
(b) the School discloses personal information to a contractor or third party, or
(c) a contractor uses or discloses personal information on behalf of the School.

7.22.2 In many cases contractors will be 'small businesses' and not subject to the Privacy Act, for example, specialist music teachers or sports coaches. Personal information will also be disclosed, on occasions, to volunteers who assist the School, who will also be exempt for the Act.

7.22.3 This means they will not need to provide any notice under NPP 1.5. If, however, personal information is disclosed to contractors which are not 'small businesses' then they, or the School on their behalf, will need to comply with NPP 1.5.

7.22.4 If the School collects personal information from a contractor, even if the contractor is not subject to the Privacy Act, then the School will need to comply with NPP 1.5. In complying with NPP 1.5 in such circumstances, the School would have to take reasonable steps to let the individual know of the matters listed in NPP 1.3. The Guidelines indicate that the steps taken to make the individual aware of the matters in NPP 1.3 will depend on the circumstances. The Guidelines also provide that 'reasonable steps' in this context includes whether a reasonable individual would expect the information to be collected indirectly. If the facts fall into this category the School may not have to do anything under NPP 1.5. The 'standard collection notice' is designed to cover this situation in most circumstances. See also paragraph 7.7 and see the 'standard collection notice' in paragraph 7.10.1.

Example:

An example of a circumstance where a School might not have to take any steps under NPP 1.5 is where a pupil is examined by a third party for psychometric testing and the pupil's Parent agrees to the third party disclosing personal information to the School. In such a case although the School is collecting personal information about a pupil from a third party, the pupil's Parent is aware that the information is being collected by the School indirectly.

7.22.5 Unless exempt from the Act, where a contractor or third party collects sensitive information from the School, then the contractor or third party will need the individual's consent under NPP 10. However, such consent can be obtained by the School on behalf of the contractor or third party. The 'standard collection notice' is designed to cover this situation in most circumstances. If, however, the School considers that a certain act goes beyond the situations envisaged in the 'standard collection notice' then the School, or the party collecting the sensitive information, should obtain the individual's consent for collection.

7.22.6 Similarly, the School will need consent from the individual if it collects sensitive information from a contractor or third party (and also comply with NPP 1.3).
Example:
An example of where this might occur is where a pupil's Parent directs a pupil's doctor to disclose to the School sensitive information about the pupil, and the School collects the information (in a record) as a result. In such a case consent to the School's collection might be implied. The 'standard collection notice' is designed to cover this situation in most circumstances. If, however, the School considers that such collection goes beyond the situations envisaged in the 'standard collection notice' then they should get an assurance from the contractor or third party that the individual has consent to the School's collection (as per paragraph 7.26.8) or otherwise obtain the individual's consent.

7.23 How to comply:
7.23.1 To facilitate compliance with the NPPs the School should specifically require their contractor in a written agreement to keep personal information they are provided about Parents and pupils confidential and only use it for the purposes of the School. The implications under the Privacy Act where the School deals with contractors is discussed further in paragraph 16.12.

7.24 Sensitive Information (NPP 10)

7.24.1 Requirement:

In general an organisation should not collect sensitive information about an individual, unless an applicable exception applies. The definition of sensitive information is set out in paragraph 2.3.1.

The exceptions include where:

(a) the individual has consented
(b) collection is required by law
(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual and the individual is incapable of giving consent or cannot physically communicate consent
(d) the information is health information and collection is necessary to provide a health service to the individual and the information is collected as required by law or by relevant established rules of a health or medical body, or
(e) other specific circumstances exist for sensitive information which is health information.

7.25 What the Guidelines say: 10.1(a) Collecting sensitive information with consent

7.25.1 The School would normally need clear evidence that an individual had consented to it collecting sensitive information. If, at the same time, the School has given the individual comprehensive information on NPP 1.3 matters, including proposed uses and disclosures, the School is likely to have a strong basis for assuming it also has the individual’s consent to such proposed uses and disclosures.

7.25.2 If the School seeks to meet an individual’s special needs, it could do this in a number of ways that do not necessarily involve collecting sensitive information. For example, it could collect information about the language the individual speaks or the individual’s specific dietary preferences or requirements rather than ask about the individual’s racial or ethnic origin or disability.
7.26 What the Guidelines say: 10.1(b) – (e) Collecting sensitive information without consent

7.26.1 An example of where an organisation might be required by law to collect sensitive information under NPP 10.1(b) would be where there is a law that requires a blood bank to collect information about an individual’s sexual practices if they wish to give blood.

7.26.2 Individual’s may be legally incapable of consenting to the collection of sensitive information about themselves for the purposes of NPP 10.1(c) because of their mental or psychological state, or their age. Individuals may be legally incapable of giving consent regardless of whether a court or competent tribunal has made a formal determination about their capacity. In the case of a young person, ability to give consent is to be determined on a case-by-case basis. An example of a life or health emergency where NPP 10.1(c) might apply is where an individual is badly injured and an organisation needs to find out an individual’s blood type.

7.26.3 A ‘non-profit organisation’ under NPP 10.1(d) means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims. If the organisation has other aims, NPP 10.1(d) does not apply.

7.26.4 An example of where NPP 10.1(e) might apply is where an individual has made a claim under their life insurance policy and the insurer is preparing to dispute the claim and it needs to collect health or other sensitive information about the claimant and about witnesses in order to prepare its case.

7.26.5 Schools are not non-profit organisations as defined in the NPPs and thus do not fall within NPP 10.1(d).

7.27 How to comply:

7.27.1 Sensitive information may be collected, among other things, if the individual consents to the collection of that information, or it is required by law. In most circumstances health information is sought to enable the School's statutory obligations to be met or to enable it to discharge its duty of care. Comments on the issue of collection of sensitive information with consent are contained are in paragraph 16.1. Consent, where needed, can be given by the Parent.

7.27.2 When collecting sensitive information, the requirements of NPP 1 must also be met. Therefore, regardless of whether NPP 10 requires that consent be obtained before sensitive information is collected, the School, for example, under NPP 1.1 must ensure that the collection is necessary for one or more of its functions and activities and under NPP 1.3 take reasonable steps to make the individual aware of a number of matters.

7.27.3 Sensitive information is collected by means other than by way of forms, such as during interviews, telephone calls, meetings and medical reports. On occasions sensitive information will be collected from third parties. To pre-empt such situations, it is important that the individual whose information is collected (eg job applicant, pupil or Parent) is made aware that their sensitive information is likely to be collected, and to obtain their consent to such collection. To achieve this a sensitive information collection notice is included in the 'standard collection notice'. It may be appropriate on some occasions to get specific consent and give a specific collection notice.

7.27.4 In some instances there is collection of sensitive information due to a legal obligation to collect such information.

Example:
Examples of collection as required by law include:
immunisation records and information requested in enrolment and various medical forms (eg as required under the public health legislation), and
certain criminal record checks (eg as required under child protection laws in some States).

7.27.5 Where collection of sensitive information is required by law, NPP 10.1(b) will permit the collection of sensitive information without consent. However, NPP 1.3(e) will continue to apply and it may be necessary to inform the individual that this information is being collected.

7.27.6 Where practicable, sensitive information should be clearly identified as being such in any records. This practice would help ensure that the persons handling the information recognise the extra confidentiality and security that should be afforded to sensitive information.

7.27.7 Information about religion, racial and ethnic origin (also sensitive information) is in a different category. If this information is collected from the individual then consent can be implied. However, if this information is collected from a third party (such as a parish priest) permission should first be sought. Consent can be obtained from the Parents on the child's behalf.

7.27.8 Where sensitive information is collected from a third party (which would usually be health information about a child) it would be sensible to include in the relevant form a statement to the effect:

'The child who is the subject of this information or the child's parent/guardian of the child has consented to its collection.'

7.27.9 This would ensure that third party providers obtain appropriate consents. However, it may not be necessary to obtain such specific consents in all cases. This is discussed in paragraph 7.21.

7.27.10 Tables 2A, 2B and 3 illustrates the steps to be followed by the School in deciding whether it can collect personal and sensitive information.

7.28 Personal Information Collection Table 2A

<table>
<thead>
<tr>
<th>Collection</th>
<th>Provider</th>
<th>Consent</th>
<th>Collection Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal information about Pupil</td>
<td>Pupil</td>
<td>Not required</td>
<td>Covered by 'standard collection notice' to Parent</td>
</tr>
<tr>
<td></td>
<td>Parent</td>
<td>Not required</td>
<td>Covered by 'standard collection notice' to Parent</td>
</tr>
<tr>
<td></td>
<td>Third party (eg doctor, principal of another School)</td>
<td>Not required</td>
<td>Covered by 'standard collection notice', or, a 'special collection notice'*</td>
</tr>
<tr>
<td>Personal information about Parent</td>
<td>Parent</td>
<td>Not required</td>
<td>Covered by 'standard collection notice' to Parent</td>
</tr>
<tr>
<td></td>
<td>Pupil</td>
<td>Not required</td>
<td>Covered by 'standard collection notice', or, a 'special collection notice', or failure to notify because of duty of care to pupil</td>
</tr>
<tr>
<td></td>
<td>Third party (eg another Parent)</td>
<td>Consent could be implied, but not always</td>
<td>Covered by 'standard collection notice', or, a 'special collection notice'</td>
</tr>
</tbody>
</table>
### Collection Table 2B

<table>
<thead>
<tr>
<th>Collection</th>
<th>Provider</th>
<th>Consent</th>
<th>Collection Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal information about Employee **</td>
<td>Employee or Third party</td>
<td>N/A - Employee Exemption</td>
<td>N/A - Employee Exemption</td>
</tr>
<tr>
<td>Personal information about Contractor / Third party</td>
<td>Contractor / Third party</td>
<td>Not required</td>
<td>Should be given unless obvious</td>
</tr>
</tbody>
</table>

**Note:** In NSW, collection of personal information about pupils and prospective pupils will be permitted without consent for the purposes of assisting the Director–General or other schools:

1. to assess whether the enrolment of a particular student would pose a risk (because of the behaviour of the pupil) to the health or safety of any person (including the pupil); and
2. to develop and maintain strategies to eliminate or minimise that risk.


**Note:** See the provisions relating to health information in Part 4. In Victoria and the Australian Capital Territory, there is no exemption for a school which collects health information about its employees. In New South Wales information about employees and prospective employees may be able to be obtained under the Children and Young Persons (Care and Protection) Act.

### Sensitive Information Collection Table 2B

<table>
<thead>
<tr>
<th>Collection</th>
<th>Provider</th>
<th>Consent</th>
<th>Collection Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive information about Pupil</td>
<td>Pupil</td>
<td>Parent to consent on behalf of Pupil</td>
<td>Covered by 'standard collection notice' to Parent</td>
</tr>
<tr>
<td></td>
<td>Parent</td>
<td>Parent to consent on behalf of Pupil</td>
<td>Covered by 'standard collection notice' to Parent</td>
</tr>
<tr>
<td></td>
<td>Third party (eg doctor, principal of another School)</td>
<td>Parent to consent on behalf of Pupil</td>
<td>Covered by 'special collection notice'</td>
</tr>
<tr>
<td>Sensitive information about Parent</td>
<td>Parent</td>
<td>Consent implied</td>
<td>Covered by 'standard collection notice' to Parent</td>
</tr>
<tr>
<td></td>
<td>Pupil</td>
<td>Consent could be implied in some circumstances, but not always</td>
<td>Covered by 'special collection notice', or, failure to notify because of duty of care to pupil</td>
</tr>
<tr>
<td></td>
<td>Third party (eg another Parent)</td>
<td>Consent could be implied (eg in case of illness), but not always</td>
<td>Covered by 'special collection notice'</td>
</tr>
<tr>
<td>Sensitive information about Employee *</td>
<td>Employee or Third party</td>
<td>N/A - Employee Exemption</td>
<td>N/A - Employee Exemption</td>
</tr>
<tr>
<td>Collection</td>
<td>Provider</td>
<td>Consent</td>
<td>Collection Notice</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Sensitive information about Contractor / Third party</td>
<td>Contractor / Third party</td>
<td>Consent implied</td>
<td>Should be given unless obvious</td>
</tr>
</tbody>
</table>

*Note:* See the provisions relating to health information in Part 4. In Victoria and the Australian Capital Territory, there is no exemption for a school which collects health information about its employees.

7.30 Collection Compliance Steps - Table 3

```
Do you need the information?  
  Yes  
    Can you reasonably collect it from the individual?  
      Yes  
        Have you issued a collection notice under NPP 1.3?  
          Yes  
            Collect  
          No  
            Issue collection notice and collect  
      No  
        Is the individual aware of NPP 1.3 matters?  
          Yes  
            Has the individual consented to collection?  
              Yes  
                Collect  
              No  
                Obtain consent or rely on other provisions of NPP10 which permit collection  
          No  
            Issue collection notice to individual or require 3rd party to do so  
  No  
    Don't Collect  
```
7.31 Do's and Don'ts for collection

**DO** only collect personal information that the School requires to carry out its functions and activities.

**DO** identify the School and its contact details when collecting personal information.

**DO** inform individuals that they can access their personal information, subject to the requirements of the Privacy Act.

**DO** inform individuals of any plans to disclose their personal information to others.

**DO** consider, and notify individuals of, all the reasons for which you are collecting their personal information.

**DO** inform individuals of the consequences, if any, if they do not provide requested information.

**DO** take reasonable steps to ensure that individuals, when you collect their personal information, are made aware of:

- the School's identity and contact details
- the individual's access rights to the information
- why the information is being collected
- to whom the information is usually disclosed
- any law requiring the information to be collected
- the main consequences (if any) if the individual does not disclose all or part of the information.

**DON'T** collect personal information from someone about another individual (e.g., next of kin details) unless it is unreasonable or impracticable for you to contact the individual directly.

**DON'T** collect personal information if you do not need it.

7.32 Additional Do's and Don'ts for sensitive information

**DO** only use sensitive information for the purposes for which it was disclosed.

**DO** ask for permission if you collect sensitive information.

**DON'T** collect sensitive information unless it is necessary.
8. USE AND DISCLOSURE

8.1 Use and Disclosure (NPP 2.1)

8.1.1 Requirement:
An organisation must not use or disclose personal information about an individual other than:

(a) for the primary purpose for which it was collected (NPP 2.1); or
(b) for a secondary purpose which is related to the primary purpose of collection (or directly related in the case of sensitive information), and which the individual would reasonably expect (NPP 2.1(a)); or
(c) with the individual's consent (NPP 2.1(b)); or
(d) for direct marketing where a number or requirements are met, including where the information is not sensitive information, the information will be used and not disclosed, it is impractical to first obtain the individual's consent, and the individual is given the right, free of charge, to 'opt-out' from receiving further direct marketing (NPP 2.1(c)); or
(e) where the organisation reasonably believes that the use or disclosure is necessary to prevent threats to life, health or public safety; or
(f) where the organisation has reason to suspect that unlawful activity is being, or may be, engaged in, and the use or disclosure of the personal information is a necessary part of its investigation or for the reporting of its concerns to relevant persons or authorities; or
(g) where required or authorised by or under law; or
(h) the organisation reasonably believes the use or disclosure is necessary for the prevention, detection or investigation of crime or other enforcement laws or for legal proceedings.

8.1.2 NPP 2.1 will permit the School to use and disclose personal information which it collects for a secondary purpose so long as:

(a) it is related to the primary purpose of collection (or directly related if sensitive information), and
(b) the use or disclosure would be reasonably expected by the subject individual.

8.2 What the Guidelines say: Primary and related purpose

Where the School collects personal information directly from the individual the context in which the individual gives the information to the School will help identify the primary purpose of collection. When an individual provides, and the School collects, personal information, they almost always do so for a particular purpose – for example, to enrol a pupil or receive a service. This is the primary purpose of collection even if the organisation has some additional purposes in mind.

How broadly a School can describe the primary purpose will need to be determined on a case-by-case basis and it will depend on the circumstances, but in a large number of instances this would be 'to provide schooling'.
Where a School collects personal information indirectly a guide to its primary purpose of collection could be what the School does with the information soon after it first receives it.

8.2.1 Related and directly related purposes within reasonable expectations

To be related, the secondary purpose must be something that arises in the context of the primary purpose.

For sensitive information the use or disclosure must be directly related to the primary purpose of collection. This means that there must be a stronger connection between the use or disclosure and the primary purpose for collection.

8.2.2 Reasonable expectation

The test for what the individual would ‘reasonably expect’ would be applied from the point of view of what an individual with no special knowledge of the industry or activity involved would expect.

8.2.3 Factors to consider

When thinking about whether a use or disclosure falls within the primary purpose or a related or directly related purpose within the individual’s reasonable expectations a School could, where relevant consider:

• the context in which it is collecting the personal information
• the reasonable expectations of the individual whose information it is
• the form and content of information the School has given about why it is collecting the individual’s information (for example under NPP 1.3 and 1.5)
• how personal, confidential or sensitive the information is, and
• any duties of care or other professional obligations a School might have (although care would be needed if these are not within the person's reasonable expectations).

8.2.4 Secondary use and disclosure with consent (NPP 2.1(c))

A School may use or disclose personal information for a secondary purpose if it has the individual’s consent. Consent to the use or disclosure can be express or implied. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the School. If the School's use or disclosure has serious consequences for the individual, the School would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In such situations it would ordinarily be more appropriate for the School to seek express consent.

8.2.5 Personal information is used and disclosed by Schools about pupils to a variety of other parties. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies NPP 2 on a case by case basis.
### Use & Disclosure of personal and sensitive information about Pupils

<table>
<thead>
<tr>
<th>Category</th>
<th>Use &amp; Disclosure of personal and sensitive information about Pupils</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary purpose</strong></td>
<td><em>Personal information and Sensitive information</em></td>
</tr>
<tr>
<td></td>
<td>• provide schooling</td>
</tr>
<tr>
<td><strong>Secondary purpose</strong></td>
<td><em>Personal information</em></td>
</tr>
<tr>
<td>(related and reasonably expected)</td>
<td>• send newsletters, magazines, mail-outs and correspondence</td>
</tr>
<tr>
<td></td>
<td>• to include in newsletters, magazines and mail-outs</td>
</tr>
<tr>
<td></td>
<td>• administration (eg records of attendance)</td>
</tr>
<tr>
<td></td>
<td>• provide reports to Parents</td>
</tr>
</tbody>
</table>

### Use & Disclosure of personal and sensitive information about Parents

<table>
<thead>
<tr>
<th>Category</th>
<th>Use &amp; Disclosure of personal and sensitive information about Parents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary purpose</strong></td>
<td><em>Personal information and Sensitive information</em></td>
</tr>
<tr>
<td></td>
<td>• provide schooling for pupil</td>
</tr>
<tr>
<td><strong>Secondary purpose</strong></td>
<td><em>Personal information</em></td>
</tr>
<tr>
<td>(related and reasonably expected)</td>
<td>• send newsletters, magazines, mail-outs and correspondence</td>
</tr>
<tr>
<td></td>
<td>• contact information</td>
</tr>
<tr>
<td></td>
<td>• for committees</td>
</tr>
<tr>
<td><strong>Secondary purpose</strong></td>
<td><em>Sensitive information</em></td>
</tr>
<tr>
<td>(directly related and reasonably expected)</td>
<td>• compliance with law (eg immunisation records, Health Department)</td>
</tr>
<tr>
<td></td>
<td>• assess eligibility and apply for funding and government grants</td>
</tr>
<tr>
<td></td>
<td>• assess and address health issues and learning difficulties</td>
</tr>
<tr>
<td></td>
<td>• provide medication and assistance when required (eg administering medication)</td>
</tr>
<tr>
<td></td>
<td>• compiling health record lists and medication lists</td>
</tr>
<tr>
<td></td>
<td>• doctor or hospital (for medical assistance)</td>
</tr>
</tbody>
</table>

#### 8.2.6
Personal information is used and disclosed by Schools about Parents to a variety of other parties. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies NPP 2 on a case by case basis.

<table>
<thead>
<tr>
<th>Category</th>
<th>Use &amp; Disclosure of personal and sensitive information about Parents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary purpose</strong></td>
<td><em>Personal information and Sensitive information</em></td>
</tr>
<tr>
<td></td>
<td>• provide schooling for pupil</td>
</tr>
<tr>
<td><strong>Secondary purpose</strong></td>
<td><em>Personal information</em></td>
</tr>
<tr>
<td>(related and reasonably expected)</td>
<td>• send newsletters, magazines, mail-outs and correspondence</td>
</tr>
<tr>
<td></td>
<td>• contact information</td>
</tr>
<tr>
<td></td>
<td>• for committees</td>
</tr>
<tr>
<td><strong>Secondary purpose</strong></td>
<td><em>Sensitive information</em></td>
</tr>
<tr>
<td>(directly related and reasonably expected)</td>
<td>• compliance with law (eg a law relating to child protection - where Parent volunteers to drive a car for an excursion)</td>
</tr>
<tr>
<td><strong>Direct Marketing</strong></td>
<td><em>Fundraising</em></td>
</tr>
<tr>
<td></td>
<td>• marketing for potential enrolments</td>
</tr>
</tbody>
</table>

#### 8.2.7
Personal information is used and disclosed by Schools about contractors to a variety of other parties. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies NPP 2 on a case by case basis.
### Use & Disclosure of personal and sensitive information about contractors

#### Primary purpose

*Personal information and Sensitive information*
- to engage the contractor

#### Secondary purpose (related and reasonably expected)

*Personal information*
- contact information
- agencies (to pay invoice)

*Sensitive information*
- Workers’ compensation reports

---

8.2.8 Personal information is used and disclosed by Schools about 'others' (eg alumni, next of kin) to (potentially) a variety of other parties. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies NPP 2 on a case by case basis.

### Use & Disclosure of personal and sensitive information about others

#### Primary purpose

*Personal information*
- next of kin
- emergency contacts

#### Secondary purpose (related and reasonably expected)

*Personal information*
- mail to alumni

---

8.2.9 In many instances of collection a separate consent is obtained, resulting in the information being used or disclosed with consent. Also, information may be used or disclosed from different two sources of personal information.

8.3 How to comply:

8.3.1 A 'standard collection notice' should help overcome the potential for confusion as for what purposes the information can be used and a resultant possible breach of NPP 2.

8.3.2 The School will need to consider amending its enrolment and employment forms through which personal information is collected, so that it includes a collection notice (see paragraphs 7.10.1 and 7.13).
8.4 Use of personal information for direct marketing purposes (NPP 2.1(c))

8.4.1 Requirement:
Personal information may be used for direct marketing without the individual's consent and even though direct marketing is not a primary or secondary purpose of collection, provided that all of the following are satisfied:

(a) the personal information being used is not sensitive information; and
(b) it is impracticable for the organisation to seek the individual's consent before that particular use; and
(c) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
(d) the individual has not made a request to the organisation not to receive direct marketing communications; and
(e) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
(f) each written direct marketing communication by the organisation with the individual sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically.

8.5 What the Guidelines say:
Organisations may use non-sensitive personal information for direct marketing where, among other things, it is impracticable to seek the individual’s consent and where the individual is told that they can opt out of receiving any more marketing communications from the organisation. This principle only applies to the use of non-sensitive information for direct marketing and does not permit a School to disclose personal information for the purpose of direct marketing.

8.5.1 Impracticable to seek consent
8.5.2 Considering whether it is impracticable to seek the individual’s consent involves balancing a number of factors that could include:

- how often the School is in contact with an individual
- the way a School communicates with an individual
- the consequences for the individual of receiving the information without having consented, and
- the cost to the School of seeking consent.

The question of impracticability would generally be considered at the time of the proposed use of the personal information for direct marketing – not the time the personal information was collected.
8.6 How to comply:

8.6.1 Reference to fundraising material is included in the 'standard collection notice'. Therefore, individuals that have been provided with the 'standard collection notice' (or are otherwise aware of its contents) should reasonably expect their personal information to be used for this related secondary purpose. However, if direct marketing communications are to be sent to people who have not been provided with the 'standard collection notice' or are not otherwise aware of its contents, then the School may need to rely on NPP 2.1(c) to send the direct marketing communications. If so, each direct marketing communication should include an 'opt-out clause' which should be brought to the individual's attention. An example would be:

Opt-out clause

If you do not wish to receive any further fundraising/direct marketing communications from us, please tick the box below and return this [form] to [us].

☐ No, I do not wish to receive fundraising/direct marketing communications.

8.6.2 We note that in the Guidelines that the Privacy Commissioner is of the view that it would normally not be impracticable under NPP 2.1(c) for the School to obtain consent to send direct marketing communications via online methods (such as by email).

8.7 Use or disclosure required by law (NPP 2.1(g))

8.7.1 What the Guidelines say:

The Privacy Act does not override specific legal obligations relating to use or disclosure of personal information. ‘Law’ includes Commonwealth, State and Territory legislation, as well as common law. If an organisation is required by law to use or disclose personal information it has no choice and it must do so. If an organisation is authorised by law to use or disclose personal information it means the organisation can decide whether to do so or not.

8.7.2 Disclosure authorised by law in NSW

In NSW, specific legislation authorises disclosure of personal information relating to a pupil, prospective pupil, staff volunteers and parents for certain child protection purposes. For detailed information see "A Guide for NSW Non-Government Schools on Reporting, Disclosing and Exchanging Personal Information for the Purposes of Child Wellbeing".

8.8 How to comply:

8.8.1 Where a disclosure is required as a result of a duty of care towards an individual, then this may be done under NPP 2.1(g), without the individual's consent. Similarly, where there is a legislative requirement to disclose information this may be done so under NPP 2.1(g) without the individual's consent.

8.8.2 Table 3 illustrates what steps should be taken by the School in deciding whether it can use or disclose personal and sensitive information.
### Use & Disclosure Compliance Steps - Table 4

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the information to be used or disclosed for the primary purpose of collection?</td>
<td>Can use and disclose</td>
<td>Do not use or disclose</td>
</tr>
<tr>
<td>Is the information to be used or disclosed for a reasonably expected related secondary purpose (or directly related if sensitive information)?</td>
<td>Can use and disclose</td>
<td></td>
</tr>
<tr>
<td>Has the individual consented to the use or disclosure?</td>
<td>Can use and disclose</td>
<td></td>
</tr>
<tr>
<td>Is the information necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety?</td>
<td>Can use and disclose</td>
<td></td>
</tr>
<tr>
<td>Is the use or disclosure required or authorised by or under law (eg an obligation of duty of care)?</td>
<td>Can use and disclose</td>
<td></td>
</tr>
<tr>
<td>Is the information not sensitive and to be used for the secondary purpose of direct marketing?</td>
<td>Can use if comply with NPP 2.1(c) conditions</td>
<td></td>
</tr>
<tr>
<td>Does any other provision in NPP2 permit disclosure?</td>
<td>Can use and disclose</td>
<td></td>
</tr>
</tbody>
</table>

© CEC & NCISA 2001
8.9 Do's and Don'ts

| **DO** | follow the School's policy regarding obtaining consent when collecting personal information. |
| **DO** | make a note of individuals who inform you that they do not wish to receive direct marketing communications. |
| **DO** | provide the School's address and phone number, and if communicating by email/fax its email/fax address, when sending direct marketing communications. |
| **DO** | use or disclose an individual's personal information which is first collected by a related School only for the same primary purpose or reasonable expected related secondary purpose of collection of the related School. |
| **DO** | make a written note of use or disclosure of personal information if used or disclosed for the prevention, detection or investigation of a crime or other enforcement laws or for legal proceedings. |
| **DON'T** | disclose personal information unless with consent, for the primary purpose of collection or for a reasonably expected related secondary purpose of collection (or *directly related* secondary purpose in the case of sensitive information) |
9. DATA QUALITY

9.1.1 Requirement:
An organisation must take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, complete and up-to-date.

9.1.2 In most cases it appears that there is no established procedure for updating records, passing on changes, or deleting records that are no longer used or required.

9.2 What the Guidelines say:
The aim of NPP 3 is to prevent the adverse consequences for people that might result from an organisation collecting, using, or disclosing inaccurate, incomplete or out-of-date personal information.

Reasonable steps to confirm the accuracy, completeness and currency of the personal information they hold only need to be taken at the time they collect, use or disclose it. The information does not need to be checked at other times. However, a School may be obliged to correct personal information it holds should the individual to whom the information relates establish that it is not accurate, complete or up-to-date (see NPP 6.5).

The main focus for Schools to comply with NPP 3 might be on areas where inaccurate, incomplete or out-of-date personal information is most likely to have a detrimental affect on individuals.

9.3 How to comply:
9.3.1 The School should establish standard procedures to ensure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

9.3.2 In respect of a regular audit of all records of personal information, the Guidelines indicate that 'reasonable steps' for the purpose of NPP 3 will vary depending on the circumstances, and factors to consider include:
(a) the likelihood of the information not being complete, accurate and up-to-date
(b) whether the information is the type that would change over time
(c) how recently the information was collected
(d) the reliability of the information, and
(e) who provided the information.

9.3.3 Therefore, the School is not necessarily required to check and re-check all records of personal information for accuracy etc in all circumstances.

9.3.4 In order to achieve compliance procedures should be adopted to ensure that:
(a) records containing sensitive information such as health information be checked for accuracy before being used or relied upon
(b) there is a regular audit of all records of personal information held, whereby records that are not used or required are disposed of and inaccurate records updated
(c) records are de-identified or destroyed when no longer needed by the School, and...
either in conjunction with the 'regular audit' or otherwise, a periodic 'mail-out' is made to the information provider providing an opportunity to update, and ensure the accuracy of, their personal information.

9.4 Sharing personal information

9.4.1 Where personal information is shared between 'related Schools' or between Schools in the same system, the disclosing and receiving School keep records as to whom the personal information was disclosed to/collected from. Once either School becomes aware of any change in the personal information then that School may then pass on such changes and corrections to the other School. This will help ensure that the information held by both Schools is consistent and remains accurate and up-to-date. See paragraph 17.1.15 regarding the related Schools exemption.

9.4.2 What procedures are put in place in this regard will likely be dependant upon the size of the School.
9.5 Do's and Don'ts

**DO** be familiar with the School's systems to ensure accurate and up-to-date personal information is kept.

**DO** consider the age of personal information, and whether the information is likely to change (e.g., an address is more likely to change rather than a name), in determining whether it is likely that the information is inaccurate, incomplete or out-of-date.

**DO**, when passing personal information internally or to a related School, notify the other party of the age of the information if this is likely to affect its accuracy and currency.

**DO** consider the impact if the information is incomplete, inaccurate or out-of-date (e.g., health information) and take appropriate steps.

**DO** investigate any clear inconsistencies with personal information held (e.g., recorded as a male, but is an ex-pupil in an all-girl school).

**DO** consider whether the information was collected directly from the individual and whether it is a reliable source.

**DO** give the individual a chance to comment on the information provided, if reasonable and practicable to do so.

**DO**, where practicable, check personal information with existing records collected for the same or a related purpose to see whether it is consistent, accurate and up-to-date before using or disclosing personal information.

**DO** try to provide individuals with user-friendly ways to update their information.

**DO** keep records accurate by notifying a related School from/to which personal information is collected/disclosed of any changes to the information, and keep a record for such notification.

**DON'T** continue to use information you believe to be out of date or inaccurate.
10. DATA SECURITY

10.1 Data Security - protection of records (NPP 4.1)

10.1.1 Requirement:
An organisation must take reasonable steps to protect personal information it holds from misuse, loss and unauthorised access, modification or disclosure.

10.1.2 The level of security should be in proportion to the level of sensitivity of the personal information. Therefore extra care must be taken to ensure that sensitive information is secure.

10.2 What the Guidelines say:
Protecting the security of personal information could consist of maintaining:

- physical security – by adopting measures to prevent unauthorised entry to premises, systems to detect unauthorised access and secure containers for storing paper-based personal information
- computer and network security – by adopting measures to protect computer systems and networks for storing, processing and transmitting personal information from unauthorised access, modification and disclosure
- communications security – by protecting communications via data transmission, including email and voice, from interception, and preventing unauthorised intrusion into computer networks, and
- personnel security – by adopting procedural and personnel measures for limiting access to personal information by authorised staff for approved purposes and controls to minimise security risks to an organisation’s IT systems.

10.3 Reasonable steps
What are reasonable steps to secure personal information will depend on the organisation’s particular circumstances. Some relevant factors could include:

- the sensitivity of the personal information the School holds
- the harm that is likely to result to people if there is a breach of security;
- how the School stores, processes and transmits the personal information (for example, paper-based or electronic records), and
- the size of the School (the larger the School, the greater the level of security likely to be needed).

10.4 How to comply:
10.4.1 The School should ensure hard copy records are secured in locked cabinets with restricted access and having building alarms or similar security measures.

10.4.2 Where there is a potential for unauthorised access to personal information, for example, health information (or any other personal and sensitive information) is displayed (eg in a staff room) or distributed to staff members, steps should be taken to ensure that unauthorised
access to that information is minimised.

10.4.3 Restricting staff room access to staff members, or discreetly positioning a notice board exhibiting health information is likely to satisfy NPP 4.1. Security of such information should be considered on a case by case basis.

Example:
If a number of Parents and pupils had access to an area which contained a list of children's names, their illnesses and medication requirements, then this would be likely to breach NPP 4.1. However, if such information were only kept in a locked safe which would be difficult to access in the event of an emergency, then this would exceed what is required under NPP 4.1. A common sense approach should prevail.

10.4.4 In relation to staff members taking records of personal information outside School grounds (eg school assignments and laptop computers), staff should be reminded about the need to keep personal information secure, especially in the case of sensitive information where the adverse consequences of unauthorised access may be high.

10.4.5 In respect of electronic records of personal information, steps must be taken to ensure that personal information contained in databases are appropriately secure. This would often include having restricted access, passwords that limit such access and other appropriate measures to prevent unauthorised access to records. Additionally, the School must continue to ensure that appropriate firewalls and other security technology is applied to protect electronic records of personal information. This will also apply to the security of electronic communications that contain personal information.

10.4.6 The presence of policies and security measures in respect of computer, email and Internet use should be reviewed. Attached in Section 20 Annexure B is a draft email and Internet policy which should be considered.

10.4.7 Appropriate warnings to staff to ensure that passwords are not divulged and that electronic records are not accessed by unauthorised means should be contained in computer or Internet use polices.

10.4.8 It must be ensured that the School has in place comprehensive confidentiality and security procedures and inform all individuals who have access to personal information (such as employees and contractors) as to the appropriate manner in which personal information should be treated.

10.4.9 These procedures should be monitored and audited for compliance to ensure their effectiveness.

10.5 Use of the Internet and emails

10.5.1 For collection of personal information through websites (where relevant), the School must ensure that the data is stored securely to prevent unauthorised access. Reasonable steps will need to be taken to ensure that information provided over the Internet, for example through online enrolments, is secure.

10.5.2 Reasonable steps must be taken so that email communications, and the personal information contained therein, are secure in order to prevent unauthorised access. Emails and website collection points will require the use of appropriate collection notices, and in the case of emails that are direct marketing communications, carry opt-out provisions.

10.6 Destruction and permanent de-identification (NPP 4.2)
10.6.1 Requirement:
Where personal information is no longer required for an authorised purpose, an organisation must take reasonable steps to destroy or permanently de-identify the personal information.

10.7 What the Guidelines say:
Reasonable steps would not necessarily involve detailed culling of existing personal information. However, if an organisation does not have in place systems for destroying or de-identifying personal information that is no longer needed, NPP 4.2 would require it to progressively develop such systems.

Destruction of records containing personal information should be by secure means. Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction and should only be used for documents that are already in the public domain. Reasonable steps to destroy paper documents that contain personal information include shredding, pulping or disintegration of paper.

The reasonableness of steps taken to destroy personal information contained in electronic records will depend on the medium on which the data is stored and the available methods for erasing data.

10.8 How to comply:
10.8.1 Personal information which is no longer required for an authorised purpose should be destroyed or permanently de-identified.

10.8.2 In determining whether information is no longer required under NPP 4.2 the School should have regard to a number of matters, including:
   (a) whether there is a legal requirement to retain the information
   (b) whether it is likely that the information will be required at a later date, and
   (c) whether destroying the information would likely have a prejudicial effect on the School.

10.8.3 Schools may also wish to discuss with their insurer and/or legal adviser what records should be kept and for how long.

10.8.4 When personal information is 'no longer required' will be a matter for the School to determine. As long as a policy to retain data can be reasonably justified there will be no infringement of this NPP. This is a risk assessment issue for the School.

10.8.5 In the event that there is a conversion of information collected from hard-copy records to electronic databases, it is important to consider whether it is possible and appropriate to destroy or permanently de-identify the information as soon as practicable after they are processed into the electronic form. In some cases this may be inappropriate.
Example:

Some Schools consider it appropriate to update incorrect information on a database but retain the original (and now inaccurate) information in the original form from which the information was initially collected. The keeping of original records in such circumstances may be appropriate where the original record is required to compare a change in an individual's medical condition, learning development or progress, or where it is necessary to retain the original record to verify what information was originally provided. However, in other cases it may be appropriate to discard information contained in a hard-copy form which has been converted to electronic form, for example a leave request form or a timesheet. However, this may depend on the situation and type of information contained in the form.

10.8.6 In cases where it is considered necessary to retain information that is old or superseded, steps must be taken to ensure that this old or inaccurate information is not confused with the new up-to-date accurate information. This is especially so where the information concerned is sensitive information and the consequence of relying on the old or incorrect information is adverse or detrimental to, or embarrassing for, the individual.

10.8.7 Further, in the case of both electronic or hard-copy records, the School must ensure that procedures are in place whereby records that are no longer required are de-identified or destroyed. The destroying information must be done by secure means (eg securely locked bins, shredding, pulping) and not by general disposal. A fixed annual review of personal information would be a way to ensure that this obligation is complied with.
## 10.9 Do's and Don'ts

| **DO** consider how, and in what form, you store personal information, and consider how secure this is. |
| **DO** ensure that all hard-copy records of personal information are kept securely locked or supervised. |
| **DO** locate personal information that is no longer needed. In such cases, the information should be destroyed or de-identified. |
| **DO** ensure that staff maintain adequate security of all personal information under their control. |
| **DO** limit access to personal information only to those who require it to carry out their duties for a permitted purpose (i.e. a 'need to know' basis). |
| **DO** contact the School's privacy contact if you are unsure as to the company's practices and procedures for keeping personal information secure. |
| **DO** make a note of to whom personal information has been disclosed, for example, a record of who has a particular file, or who has access to a particular database. |
| **DO** scrutinise requests for disclosure of personal information, for example follow the School's procedure to identify an individual who asks you to disclose or 'check' their personal information. |
| **DO** ensure that in cases of shared computer, that tools are implemented to avoid possible privacy breaches. |
| **DO** ensure that staff login and out in accordance with allocated level of access. |
| **DON'T** access, discuss, display, or disclose personal information other than as permitted by the NPPs. |
| **DON'T** leave personal information unattended and not specially secure. For example, if you leave your computer for an extended period of time, shut it down, log off or use a screensaver with password. Don't leave files where they may be access by unauthorised people. |
| **DON'T** ever allow unauthorised access, modification or disclosure of personal information. |
11. OPENNESS - PRIVACY POLICY

11.1 Openness - Privacy Policy (NPP 5)

11.1.1 Requirement:
An organisation must set out in a document clearly expressed policies on its management of personal information and must make that document available to anyone who asks for it. (NPP 5.1)

In addition, an organisation must, on request, take reasonable steps to let an individual know, in general terms, what sort of information is held and why, and how it collects, holds, uses and discloses that information. (NPP 5.2)

11.1.2 It is important that a Privacy Policy (or similar document) be made widely available (including to employees and contractors). In addition, it is important that where policies are in place (eg policies in respect of confidentiality or Internet and email usage) that these policies are adequately enforced.

11.2 How to comply:

11.2.1 Adopt a Privacy Policy which expresses, in plain language, the School's policy or policies on its management of personal information.

11.2.2 A draft Privacy Policy is attached which covers the following issues:
(a) the NPPs
(b) sharing and disclosing information (internally, to 'related Schools', to third parties)
(c) direct marketing
(d) the transfer of information overseas, and
(e) any exemptions in the Privacy Act that apply.

11.2.3 The policy we have drafted is intended to comply with NPP 5.1 and contain the information required for Schools to comply with NPP 5.2. Also, the policy is broadly intended to contain the information required by NPP 1.3.

11.2.4 This policy can be adapted as required by the School. Not only would this policy be used to help inform individuals about the practices of the School in relation to personal information, but it would also serve as a guide to the School's staff as to the standard to be applied in respect of handling personal information and ensure consistency in the School's approach to information privacy.

11.3 Educating Staff

11.3.1 The key to achieving compliance and ensuring continued compliance with the Act will be through the conduct of the School's employees and other staff members. Consequently, the School's staff members must be educated to a certain degree about the requirements of the Act.

11.3.2 There are a number of ways that employees and other staff members be made aware of the requirements of NPP 5 (and the other obligations under the Act). These include raising general awareness by:
(a) circulating the Privacy Policy to all staff
(b) informing staff on the requirements of confidentiality and by extending this obligation contractually where necessary, and
(c) holding internal seminars and workshops.

11.4 Do's and Don'ts

**DO**, if asked, inform people about the type of personal information that is being collected and why.

**DO** encourage people (eg parents, other staff members) to read the School's Privacy Policy and make them aware of how they can get a copy (eg hardcopy, web site).

**DO** make individuals aware of the School's standards and practices of using and disclosing personal information.

**DO** ensure you read the School's Privacy Policy and contact the privacy contact if you do not have a copy or do not understand anything in the Privacy Policy.

**DO** be aware that the School's Privacy Policy may change over time, and therefore take time to read the latest copy.

**DO** notify your privacy contact/Principal if you are aware of a practice in the School relating to personal information which is different from, or is not covered in, the School's Privacy Policy.

**DO** refer all queries about the Privacy Policy to the School's privacy contact.
12. ACCESS AND CORRECTION

12.1 Access and Correction (NPP 6)

12.1.1 An organisation must on request provide the individual with access to his or her own personal information and correct any inaccuracies.

12.1.2 However, there are some exceptions, including where:
- this would unreasonably impact on the privacy of other individuals (NPP 6.1(c));
- the request is frivolous or vexatious (NPP 6.1(d));
- the information relates to existing or anticipated legal proceedings between the parties, and the information would not be accessible through discovery (NPP 6.1(e));
- access would reveal the intentions of the organisation in relation to a negotiations with the individual is such a way as to prejudice those negotiations (NPP 6.1(f));
- this would be unlawful (NPP 6.1(g));
- denying access is required or authorised by or under law (NPP 6.1(h));
- providing access is likely to prejudice an investigation of possible unlawful activity (NPP 6.1(i));
- providing access is likely to prejudice the presentation, detection, investigation, prosecution or punishment of an unlawful activity, the activities of a law enforcement agency or legal proceedings (NPP 6.1(j));
- providing access is likely to reveal evaluative information generated within the organisation in connection with commercially sensitive decision-making processes (NPP 6.2).

12.1.3 Where access is desired, the organisation must, where reasonable, consider whether the use of intermediaries would allow sufficient access (NPP 6.3).

12.1.4 Reasons must be given where access is denied (NPP 6.7).

12.2 What the Guidelines say:

Access can be achieved by:
- providing the individual with a copy of the information
- letting the individual make notes of the contents of the record
- give the person a print out of the information if it is in electronic form, and
- giving the individual a summary of the information.

12.2.1 6.1(c) Unreasonable impact on the privacy of others

Access to a document containing personal information about people other than the individual requesting access need not be denied altogether. For example, in such a case, it may be possible to delete the other individual’s personal information from the document before it is released to the individual who made the request.

Information that could have an unreasonable impact on another person’s privacy can include more than information such as name and address. It could include any information in the document from which the identity of the person could be reasonably ascertained.
6.1(d) Frivolous or vexatious requests
Frivolous and vexatious requests could include those that are:
• trivial and made for amusement’s sake
• made as a means of pursuing some unrelated grievance against the organisation, or
• repeated requests for access to the same personal information.

6.1(g) Access would be unlawful
This exception would cover circumstances where providing access to personal information would be a breach of confidence under the law, for example a breach of legal professional privilege.

6.1(h) Denial of access is required or authorised by law
The law in question might be State, Territory or Commonwealth law. If an organisation is required by a law to refuse access it has no choice. It must refuse access. If an organisation is authorised by law to refuse access it means the organisation can decide whether to do so or not. The authority is there but the organisation can decide.

How to comply:

12.3.1 The School should establish a standard procedure whereby individuals are permitted to 'access' their records except where an exception to the 'access' principle applies. The School is entitled to make a charge for access on a cost recovery basis.

12.3.2 The School should ensure that it has systems in place to meet access requests and determine whether access should be granted. Access requests could be made through the School's privacy contact or the Principal.

12.3.3 Although individuals are not required to give a reason to access their records, Schools to whom access requests are made should ask the individual what information he or she wants access to, or the type of information the individual wants access to. This is likely to help facilitate the individual accessing the information he or she is seeking.

12.3.4 NPP 6 only gives individuals the right to access personal information which the School holds about that individual. It is important to note that the School to whom an access request is made should take adequate steps to identify the individual requesting access. This may include verifying that an individual has been given authority to access personal information on behalf of another individual. Such steps are likely to vary on a case by case basis. However the School should adopt the view that in most cases Parents may have access to records relating to their child unless special circumstances arise.

12.3.5 NPP 6.7 requires that organisations must provide reasons for denial access or a refusal to correct personal information. Although not required by NPP 6, it would be prudent to provide written reasons for denying access, and to retain a copy, to help avoid any confusion in the event of a dispute.

Example:
An example of being permitted to refuse access is where a 'Report by Pupil Form' in relation to an incident is not to be made available to 'other' pupils. This could possibly include pupils who are the subject of the incident and report (eg in the case of bullying).

In such a case an exception to NPP 6 may apply which would permit the School refusing or restricting access to the record (eg NPP 6.1(c) - where providing access would have an unreasonable impact on the privacy of others, or NPP 6.1(i) - where the report was a result of unlawful behaviour). In these scenarios, the School must provide reasons for denying
access. The reasons may be framed so not as to defeat the purpose of denying access (eg so as not to highlight to a 'suspect' requesting access that an investigation into their activities is underway and providing access to their personal information would prejudice the investigations).

12.3.7 It is important to note that 'law', particularly as it relates to NPP 6.1(g) and NPP 6.1(h), includes the common law. Therefore where a common law duty of care or obligation of confidence exists, it might be possible to restrict access under NPP 6.

12.3.8 Common law duties are discussed in paragraph 16.2.

12.4 Correction requirements

12.4.1 The School must take reasonable steps to correct a record of personal information it holds if the individual concerned is able to establish that the information is not accurate, completes and up-to-date.

12.4.2 However, if there is a disagreement as to whether an individual's information is accurate, complete and up-to-date and if the individual requests it, the School must take reasonable steps to associate a statement about the individual's claim with the information.

12.5 Particular Issues

12.5.1 Various issues might arise where a pupil seeks access (under NPP 6) to their personal information which is contained in records held by the School. Where a record of personal information about a pupil contains information which would normally not be released, the School would need to consider whether it may restrict access under NPP 6.

12.5.2 Examples of scenarios where a School might consider restricting access might include where the information is contained in:

(a) a psychiatric report (eg pupil exhibits anti-social behaviour)
(b) a psychometric test (eg indicating that the pupil has the mental capacity of a 9 year old when the pupil is 15 years old)
(c) a confidential communication between the School and a Parent about their child who is a pupil of the School, and
(d) Scholarship exam results, internal marks, teachers' notes.

12.5.3 Where access to the information may adversely impact on the pupil the School might consider whether NPP 6 permits the restriction of access.

12.5.4 Some of the exceptions which the School might consider relying on include where:

(a) providing access would have an unreasonable impact on the privacy of others (NPP 6.1(c))
(b) denying access is authorised by law (eg a common law duty of care) (NPP 6.1(h)), and
(c) where providing access would reveal evaluative information generated with the School in connection with a commercially sensitive decision-making process (NPP 6.2).

12.5.5 If a Parent of the pupil seeking access does not consent to their child having access this should also be considered.
12.6 Steps to Consider When an Access is Requested

12.6.1 Usually records of personal information which the School creates will be the property of the School.

12.6.2 The following are a number of matters the School might consider when an access request is made:

- If the information was collected by the School before 21 December 2001 (and not subsequently updated, used or disclosed), then NPP 6 will not apply and access may be denied
- Consider what information the individual wants access to (this may help determine whether an exception to access in NPP 6 applies)
- Consider whether NPP 6 permits the School to refuse access
- There are various forms of access (see Information Sheet 4 released by the Office of the Federal Privacy Commissioner), including:
  - allowing the individual to inspect the information
  - providing the individual a photocopy of the information
  - letting the individual take notes of the information
  - providing a print out (if the information is in electronic form) to the individual, or
  - giving the individual an accurate summary of the information
- A charge for access may be made, but it must not be excessive.
12.7 Do's and Don'ts

**DO** allow individuals to have access to, and copies of, their personal information, except where denial is permitted.

**DO** establish the identity of the individual before you provide access to personal information.

**DO** provide access to personal information in a timely manner.

**DO** contact the School's privacy contact if you think you should deny access or refuse correction to an individual's personal information and ask the privacy contact to check the reasons you are giving.

**DO** encourage individuals to notify you if they consider the personal information you hold about them is not accurate, complete and up-to-date.

**DO** inform people of their right to access their information. This must be done when collecting personal information.

**DON'T** provide an individual direct access to information if that access would unreasonably impact on the privacy of others, for example if the record contained the personal information of a number of people. Providing access to part of the records may be appropriate in such cases.

**DON'T** assume that you have to provide an individual with direct access to information if it would reveal a commercially sensitive decision-making process. Instead, **DO** provide the individual with indirect access (e.g. by extracting the raw data).

**DON'T** refuse an individual access to their personal information just because it may be costly, inconvenient or difficult to provide access.
13. IDENTIFIERS

13.1 Identifiers (NPP 7)

13.1.1 Requirement:

NPP 7 requires that identification devices provided by a government agency, such as a Medicare number, a Social Security number or a tax file number, cannot be used by an organisation as its own identifier to identify an individual.

13.2 What the Guidelines say:

NPP 7 seeks to ensure that increasing use of Commonwealth government identification does not lead to a de facto system of universal identity numbers, and to prevent any loss of privacy from the combination and re-combination of the data.

For these reasons tax file number legislation already restricts the way an organisation can collect, use or disclose a tax file number.

A Commonwealth government identifier is a unique combination of letters and numbers, such as a Medicare number, which Commonwealth government agencies or contracted service providers allot to an individual.

NPP 7 does not apply to an individual's name, an ABN or State Government identifies such as driver's licence numbers.

13.3 How to comply

13.3.1 The School must ensure that it does not adopt as its own identifier an identifier that has already been assigned to an individual by an agency.

13.3.2 Additionally, when using or disclosing identifiers, such as a Medicare number, the School must ensure that such use or disclosure is permitted by NPP 7 (eg to fulfil its obligations to the relevant agency, or to prevent threats to life, health or public safety). The School should ensure that:

(a) staff are not able to enter a person's Medicare or staff member's TFN into a database and retrieve their record, and

(b) where this search exists, the databases are modified to remove it.

13.4 Do's and Don'ts

DO use identifiers which are created by the School to identify individuals.

DON'T collect or use agency identifiers, such as an individual's Medicare number, Passport number and Social Security number, unless it is necessary to fulfil an obligation to the agency or any of NPPs 2.1(e) to NPP 2.1(h) apply.
14. ANONYMITY

14.1 Anonymity (NPP 8)

14.1.1 Requirement:
Wherever lawful and practical, individuals must have the option of not identifying themselves when entering into transactions with an organisation.

14.2 What the Guidelines say:
Unless there is a good practical or legal reason to require identification, organisations must give people the option to operate anonymously.

Anonymity is an important element of privacy. In some circumstances, it will not be practicable to do business anonymously. In others there will be legal obligations that require identification of the individual. This principle is not intended to facilitate illegal activity.

14.2.1 The Guidelines do not provide any guidance as to what 'entering into transactions' or what 'operate' in this context means.

14.3 How to comply:
14.3.1 The School should (where lawful and practicable) provide an option for individuals to remain anonymous when entering into 'transactions' with them. Most 'transactions' would require a person's details. Examples of where individuals would be able to remain anonymous would be:

(a) a one-off transaction where the individual is able to pay in cash in advance or on delivery and would only need to disclose a delivery address and perhaps a first name
(b) where an individual requests a prospectus and it can be provided without collecting the individual's personal information (eg at an 'open day'), and
(c) where surveys are conducted where there is no need to collect a respondent's personal information such as their name and address.

14.3.2 It would appear that the conduct of surveys and the issuing of questionnaires would unlikely be classified as 'entering transactions with an organisation', and therefore not within the scope of NPP 8.

14.3.3 As most 'transactions' would require a person's details, it would appear that NPP 8 is of little significance to most Schools.
15. **TRANSBORDER DATA FLOWS**

15.1 Transborder Data Flows (NPP 9)

15.1.1 Requirement:
An organisation may transfer personal information outside of Australia, other than internally within its organisation or to the individual concerned, only in limited circumstances.

The circumstances include where:

(a) the organisation reasonably believes the recipient of the information is subject to similar requirements regarding protection of personal information, or
(b) the individual consents to the transfer, or
(c) the transfer is necessary for the performance of a contract between the organisation and the individual or the individual and a third party, or
(d) the transfer is necessary for the implementation of pre-contractual measures taken at the individual's request, or
(e) the transfer is for the benefit of the individual, it is impractical to obtain the individual's consent and, if it were practical to obtain consent, the individual would be likely to consent, or
(f) the organisation has taken reasonable steps to ensure that information transferred will not be held, used or disclosed by the recipient in a manner inconsistent with the NPPs.

15.2 What the Guidelines say:

NPP 9 outlines the circumstances in which an organisation can transfer personal information it holds outside Australia. NPP 9 is based on the restrictions on international transfers of personal information set out in the European Union Directive 95/46.

In the simplest terms, NPP 9 prevents an organisation from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual’s consent or some other circumstances including where:

- the transfer is for the benefit of the individual and the organisation can show grounds for a belief that if it were practicable to obtain consent the individual would be likely to give it, or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party.

15.3 How to comply:

15.3.1 In circumstances where personal information is likely to be transferred overseas, the School transferring the information must have procedures in place for ensuring that requirements contained in NPP 9 are complied with.
15.3.2 Compliance with NPP 9 could be achieved if the relevant School:

(a) reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which upholds the NPPs. This could be achieved where personal information is disclosed to an organisation situated, for example, in a member country of the EU which has privacy laws offering similar protection to those contained in the NPPs

(b) enters into a contract with each recipient of the information which contains obligations and undertakings from the recipient that the information will be dealt with in a manner that complies with the NPPs, or

(c) obtains a consent from the individual to the transfer. All forms whereby personal information is collected could be amended to include the 'standard collection notice' and the following additional notice:

15.3.3 The most practicable course would be to provide a 'transfer overseas notice'.

**Transfer overseas notice**

We may transfer any or all of this information to a third party, whether within Australia or overseas, for the following purposes [insert purpose eg to provide information about the School].

15.3.4 A number of pupils attending various Schools are full fee paying overseas pupils (i.e. the pupils' Parents are located overseas).

15.3.5 If a Parent has received a 'standard collection notice', and the personal information about their child is transferred directly to them, then it can be contended that consent to the transfer would be implied. Therefore, the transfer will be permitted under NPP 9.

15.3.6 If the transfer is not directly to the Parent (eg it may be via a third party intermediary), the School would have to rely on another 'exception' under the NPP 9 restrictions if consent is not sought. For example, it might be argued that NPP 9.1(c) could be relied on (this 'exception' permits the transfer of personal information overseas if the transfer is necessary for the performance of a contract between the individual (i.e. the Parent) and the School). In such circumstances the School should obtain the Parent's consent to the transfer to avoid doubt.

15.3.7 An example where a transfer of information overseas may occur is where a pupil goes overseas as part of an exchange program and personal information is transferred overseas as a result.

15.4 **Do's and Don'ts:**

DO take care when transferring information overseas.

DO investigate the privacy obligations of overseas recipients of personal information, rather than simply taking their word for it.

DO observe the School's requirements in relation to the transfer of information overseas.
PART 3

16. SPECIAL ISSUES FOR SCHOOLS

16.1 Consent and Young People

16.1.1 The NPPs do not differentiate between children of different ages and thus it is difficult to determine when it is appropriate to seek consent from pupils. However, the Privacy Act does not distinguish between adults and children and thus clearly envisages that young people are to be afforded rights in respect of their privacy.

16.1.2 The Privacy Commissioner states at page 15 of the Guidelines:

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. Determining the decision-making capabilities of a young person can be a complex matter, often raising other ethical and legal issues. Organisations will need to address each case individually.

As a general principle, a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed.

In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person; for example if the child is very young or lacks the maturity or understanding to do so themselves. It should be noted that in some states, contracts with people under the age of 18 are not valid.

It may be desirable for organisations that target children or young people to specifically address issues of consent and rights of access to the personal information of children and young people in the information policy that NPP 5 requires them to have. Such a policy might contain general guidelines about how the organisation will make decisions relating to young people and children and the factors it will take into account. The policy might also deal with parental involvement, particularly factors that would indicate that a parent should be involved in the decision-making process.

16.1.3 In approaching the issue of privacy for Schools it is important to remember that the underlying arrangement between the School and Parents is contractual. Parents are engaging the School to provide schooling for their child on the terms agreed by the parties. The School's authority over the child derives from the contract with the Parents and its duties at law.

16.1.4 A Parent is recognised by the common law as having the right to make decisions concerning the child's education and to bring up their child in the religion of their choice. In all States of Australia the age of majority is 18 years.

16.1.5 For these reasons, one approach would be for the School to adopt the view that in many circumstances the contract with the Parents will govern their relationship with the child in relation to privacy, and thus consents given by Parents will act as consents given on behalf of the child and notice to Parents will act as a notice given to the child.

16.1.6 However, this approach will not be appropriate in all circumstances. A School should recognise that young people do have rights under the Act and in some circumstances it would be appropriate to seek consents from them, particularly when they are older. No doubt in most cases decisions whether to seek information or consents from pupils or from Parents is likely to follow current practices. Thus, for example, where a pupil puts his or her name down to take part in a team, the pupil would usually be impliedly consenting to it being...
disclosed to a relevant party to enable him or her to compete. As a pupil reaches greater maturity the more important it will become to consider whether it is a Parent which should be asked for consent or the pupil. Hopefully in most cases common sense will provide the answer.

16.1.7 For example, in most cases it would be appropriate for the School to collect from a mature pupil personal (and sensitive) information about the pupil gained through an interview with the pupil. Also, there will be many instances throughout a pupil's schooling where it would be impracticable and inappropriate to first obtain a Parent's consent when collecting personal information from a pupil (eg during day to day classroom activities). In respect of collecting personal information about pupils from Parents, it is suggested that it is sufficient if Parents be given a collection notice informing them of the requirements set out in NPP 1.3 and pupils do not have to be specifically informed.

16.1.8 Another potential concern is that pupils may attempt to claim a right to prevent disclosure of personal information to a Parent, such as their School report. The 'standard collection notice' seeks to overcome this by informing Parents that the School will disclose personal information about a pupil to the pupil's Parents. Where a pupil attempts to restrict disclosure of personal information (such as a School report) to a Parent, the School can argue that the disclosure is a permitted purpose. This does not prevent the School exercising its discretion to restrict disclosure of the personal information.

16.1.9 In relation to pupils seeking access (under NPP 6) to their personal information which is contained in records held by the School, see paragraph 12.5.

16.2 Duty of Care and obligations of Confidence

16.2.1 The Guidelines state that 'Law' in the context of 'required or authorised by law' under NPP 2.1(g), includes common law. The common law imposes a duty of care on Schools which they must exercise in relation to pupils and staff. It can be contended that Schools are required by this common law (duty of care), to collect certain personal and sensitive information in order to comply with this duty. This would justify the School collecting sensitive information about pupils and possibly others (eg Parents, contractors etc) under NPP 10.1(b) in order to fulfil its duty of care in its responsibility as the carer and educator of children (and others).

Example:
An example of where duty of care may require disclosure would be where a School informs a third party in temporary charge of a pupil that the pupil suffers from a particular health problem.

16.2.2 The common law, in some situations, imposes upon people an obligation of confidence. In broad terms confidence can be claimed where information is:
(a) by its nature confidential
(b) communicated in circumstances importing an obligation of confidence, and
(c) disclosure of it would be unauthorised by the provider or by law.

16.2.3 The latter requirement makes it doubtful whether the law in relation to breach of confidence would of itself permit the School to refuse access to personal information held about a person as the NPPs would appear to require personal information to be disclosed except where a specific exception applies.

16.2.4 The uncertainty in this area only serves to underline the fact that records of confidential information should only be made where there is a need to do so and in the knowledge that access to the record may be sought.
A common law duty of care and obligation of confidence might be used to restrict an individual access to records of personal information held about them in some cases.

**Example:**
An example of when confidential information may be withheld may be where a pupil has advised a teacher of a particular home situation where disclosure to the Parent the subject of the information may cause adverse repercussions for the pupil. This is not because it was confidential so much as because of the School's duty of care to the pupil. It may also have an unreasonable impact on the privacy of the pupil (NPP 6.1(c)).

16.3 Passing Information in a School Community

16.3.1 Schools like to see themselves as 'communities'. The School community will typically consist of staff, pupils, Parents, past pupils and benefactors. Where the School is affiliated with a particular religion, a minister, the church and the congregation will often be included in the broader school community.

16.3.2 As in any community, information about others is passed on through the community and on occasions will be recorded. Thus a note from a School Principal (which would constitute a 'record' when filed) to a priest that a child or child's Parent is sick would not be unusual. Technically this could not be done without the consent of the Parent. However, if the Principal is confident consent would be given, or indeed his passing on the information would be expected, then failure to adhere to the 'letter of the Principals' would be unlikely to have any repercussions.

16.3.3 In the same vein, praying for a sick child or sick Parent may involve a 'technical breach' of the NPPs if it involved disclosure of sensitive information, provided it was contained in a record, but is unlikely to cause offence. However, on occasions it may, particularly if the individual wished their illness to be confidential.

16.3.4 It should also be borne in mind that where such practices are well known in the community, consent to collection may well be implied in many circumstances and disclosure may be a reasonably expected related (or directly related) purpose of obtaining the information.

16.3.5 The guiding principle in such cases is to show sensitivity in exercising a judgement as to when it is appropriate to disclose this type of information.

16.4 Religious Information

16.4.1 Where religious information about an existing or potential pupil or Parent is sought from a minister, it would be wise to obtain consent. This can be achieved in appropriate applications or enrolment forms.

16.5 Fundraising

16.5.1 Disclosure of information for fundraising purposes raises greater difficulty. However, it is suggested that non-government schools rely on extra funds raised by approaches to Parents and Alumni and this would be a reasonably expected related secondary purpose. However, to ensure that it is expected it would be wise to include it in a collection notice. This activity is referred to in the 'standard collection notice in paragraph 7.10.1.

16.6 Passing personal information to other Schools

16.6.1 Where another School which is not within the same system or is not a related corporation requests personal information about a pupil at a School, in usual circumstances this information should not be passed on without consent. It may be done on occasions as part of the School's duty of care. Schools which are related organisations may share personal
information other than sensitive information, subject to restrictions on its use,

16.6.2 From 1 January 2006, the Interstate Student Data Transfer Note (ISDTN) and Protocol was established under the Schools Assistance (Learning Together Through Choice and Opportunity) Act 2004. The purpose of the initiative, between the Australian Government, State and Territory Education Departments, and the independent and Catholic education sectors, is to allow for the transfer of student information between schools when children move from one state to another and to provide 'flags' for the new school regarding educationally significant information about the student.

16.6.3 Under the ISDTN and Protocol, when a new student from another state enrols or applies for enrolment, the new school will follow a process to request the transfer of information from the student's previous school. The key aspect of this system is the circumstances in which the parent or student is required to give consent.

16.6.4 The ISDTN and Protocol set out the processes by which schools must obtain consent from the parent/guardian and in some cases, the student, before information can be collected from the student's previous school.

16.6.5 The consent regime is as follows:

(a) where the information is to be passed from one non-government school to another, parent or student consent is not required before the information can be passed if the previous school has a data collection notice which conforms to the notice at paragraph 7.10.1 of this Manual;

(b) where the information is to be passed from a government school to a non-government school, the new school must collect consent before requesting the information from the previous school; and

(c) where the information is to be passed from a non-government school to a government school, the obligation falls on the new school to collect the consent before it can request the information from the previous school.

16.6.6 Information about the ISDTN and Protocol and the relevant consent forms can be found at the website of the Ministerial Council on Education, Employment, Training and Youth Affairs (MCEETYA) at http://www.mceetya.edu.au/mceetya/.

16.7 Disclosure of information in NSW

16.7.1 In NSW following legislation may permit or require personal information about students, staff, parents or others.

- Children and Young Persons (Care and Protection) Act 1998;

- Education Amendment (School Attendance) Act 2009;

- Ombudsman Act 1974;

- Part 5A of the Education Act 1990 (Health and Safety risks of schools arising from student behaviour); and


A summary of the relevant provisions of these Acts is contained in "A Guide for NSW Non-Government Schools on Reporting, Disclosing and Exchanging Personal Information for the Purposes of Child Wellbeing".

16.8 School Directories

16.8.1 School directories and class lists which contain students' and Parents' name and contact
numbers, and class lists contained similar information and will involve the disclosure of personal information to others. Such a use of individuals' personal information may not be reasonably expected by the individual concerned. To avoid any doubt Schools should obtain the consent of Parents (on their own and their child's behalf) to place their details in the School Directory or class list. Alternatively, the School could notify Parents (and children) about such practices in a 'standard collection notice' (see paragraph 7.10.1).

16.9 Personal information not in a 'record'

16.9.1 The NPPs apply to personal information which is being collected for inclusion in:
(a) a 'record' (eg collecting personal information through an enrolment form), or
(b) a 'generally available publication' (eg a magazine, newsletter or information published on the Internet).

16.9.2 The NPPs also apply to personal information which has been collected and is contained in a record (eg a name and address on a pupil's file).

16.9.3 What is meant by 'record' is discussed in paragraph 2.5.

16.9.4 Under the Privacy Act a 'record' does not include many things, including:
(a) a generally available publication, and
(b) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

16.10 School Publications

16.10.1 School publications, such as newsletters, magazines and alumni publications usually contain personal information obtained either from the relevant individual or from other sources. These publications could be said to be 'generally available publications', even if the School only distributes these publications within the School community, provided they could be made available to the public on request. The effect of this is that although the information may be a 'record' when collected, it can be freely used and disclosed through dissemination of the publication.

16.10.2 Ideally, personal information which is collected for inclusion in a School publication should be collected directly from the individual, particularly where the information relates to personal or private matter. See paragraph 7.20.2 on this point. Where this is impracticable, the NPPs require that the individual be made aware of the NPP 1.3 collection information. This would generally be achieved by sending the individual a copy of the publication.

16.10.3 An alternative would be to seek to rely on the journalism exception. However this would require the School to subscribe to a set of 'standards' that deal with privacy in the context of a media organisation. Consideration is being given to establishing these standards.

16.11 Library Collections

16.11.1 The Privacy Act excludes 'anything kept in a library' from the definition of 'record'. Thus the NPPs do not apply to material contained in library collections.

16.12 Systems and Schools Conducted by Church Bodies

16.12.1 The non-government school sector includes a large number of systems. These are predominantly Catholic education systems, although a number of other religious denominations conduct schools as part of a 'system'.

16.12.2 The system model may involve the conduct of a number of schools by the one legal entity (which is generally the Catholic model) or the conduct of a number of schools which have separate legal entities but 'report' to a central authority and are ultimately subject to its
direction. In both cases many functions are centralised.

16.12.3 A Diocese is not a 'related body corporate' of another Diocese, as this term is confined to the definition contained in the Corporations Act. Each Diocese is incorporated by Act of Parliament and is created as a separate legal entity.

16.12.4 Where a system consists of separate legal entities then these will be separate organisations. In some cases they also may be related bodies corporate.

16.12.5 Personal information can be used within a system where there is one legal entity, or within a system which consists of related bodies corporate, for the purpose for which it is collected. However, where employment information is transferred to another organisation, the employee exemption will not apply to that record in the hands of that other organisation. See also Section 16.13.

16.12.6 Roman Catholic Orders that conduct Schools are generally incorporated under State Act and their affairs are managed by Trustees. In these circumstances they are not 'related bodies corporate' to other Catholic Orders within the meaning of the Corporations Act. Nor are they related to the various Catholic Dioceses.

16.12.7 When a School is not related to a second School it cannot rely upon the section 13B of the Privacy Act to disclose information to that second School. However, it can still use the provisions relating to consent or related and reasonably expected secondary purpose. In most cases the practical outcome will not be different.

16.13 Privacy Implications for Schools Dealing with Contractors

16.13.1 The following information is based on, and adapted from, Information Sheet 8 released by the office of the Federal Privacy Commissioner.

**Contractors**

16.13.2 Schools sometimes enter into contractual relationships with another party (the contractor) in which the contractor:

(a) supplies services to the School, or

(b) supplies services to someone else on behalf of the School, and

the contract involves the contractor handling personal information.

16.13.3 The Privacy Act treats the acts and practices of employees (and those 'in the service of' an organisation) in performing their duties of employment as those of the School. Contractors performing services for School are not considered to fall within this provision. However, where there is a particularly close relationship between the School and a contractor it may mean that the actions of the contractor could be treated as having been done by the School.

16.13.4 The following information covers situations where the School and the contractor would be regarded under the Privacy Act as separate entities.

16.13.5 In practical terms there may be little difference in these two situations in what the School needs to do to meet its obligations.

**Contracting with businesses not covered by the Privacy Act**

16.13.6 An important consideration for a School entering into a contract described above will be whether the Privacy Act covers the contractor. For example, the contractor may be a small business and be exempt from having to comply with the NPPs. See paragraph 7.22.1.

**Disclosure to Contractors**

16.13.7 Where the School and a contractor are separate entities under the Privacy Act where the School gives personal information to a contractor it disclosed information and the contractor
collects the information. In practical terms, this means that the School may need to have clauses in the contract for the protection of personal information it discloses to the contractor, in order to meet its obligations under the NPPs.

16.13.8 When the School contracts out functions or activities, both the School and the contractor have obligations under either NPP 1.3 or NPP 1.5 to take reasonable steps to make an individual aware of certain information. These are covered separately below.

The Contracting Organisation (School)

16.13.9 Where the School usually discloses personal information to a contractor, the school must take reasonable steps to ensure that the individuals from whom it has collected information are made aware of these disclosures (NPP 1.3(d)). The steps the School takes to inform individuals that personal information about them will be disclosed to contractors will depend on the circumstances. It may be enough to include in the collection notice a statement that "The School occasionally uses contractors to assist the School in its functions and discloses relevant personal information to these contractors to enable them to meet their obligations."

16.13.10 What other details about the contractor and relevant to NPP 1.3 the School makes an individual aware of will also depend upon the circumstances including what the School and the contractor have agreed between them. However such arrangement must not detract from the individual's privacy rights.

The Contractor

16.13.11 There are a number of ways in which a contractor collecting personal information under a contractual arrangement could meet its obligations under NPP 1.5 (to take reasonable steps to make individuals aware of NPP 1.3 matters). What are reasonable steps will depend on the circumstances. The contractor does not necessarily need to notify individuals itself. The origination that originally collects the personal information (eg the School) could notify individuals that information about them will be disclosed to the contractor, and other relevant details including the purpose for which the contractor will use the information, and how individuals can contact the contractor.

16.13.12 In some cases it could be reasonable for no steps to be taken under NPP 1.5. An example of this could be where all of the following apply:

(a) the provisions of the contract have very strong and comprehensive privacy provisions that place stringent obligations on the contractor
(b) where the organisation is prepared to monitor the contractor to ensure that it complies with the NPPs, and
(c) the organisation is prepared to take ultimate responsibility for any breach of privacy the contractor commits (although it could still seek indemnity from the contractor).

Collecting Sensitive Information Under a Contract

16.13.13 A contractor that collects sensitive information would need to have the individual's consent.

NPP 2 Use and Disclosure

16.13.14 Where the School's proposing to disclose personal information under a contract it would need to consider how NPP 2 applies to the disclosure. In some situations where the School contracts out a function or activity, the disclosure will be for a primary purpose of collection or an activity that is related to the primary purpose and within the individual's reasonable expectations (eg mailing activities).

16.13.15 Where the School discloses personal information to a contractor to carry out activities that fall outside these categories then in most cases the organisation would generally need the individual's consent under NPP 2.1(b). For example, the School will need to get consent if it proposes to disclose personal information to a contractor for the purpose of carrying out
marketing activities that are unrelated to the primary purpose of collection and outside the individual's reasonable expectations.

16.13.16 One way of reducing this risk is to ensure that the contract includes very clear provisions about the purpose for which the contractor is to use the information and other provisions necessary to ensure the contractor does not make unauthorised disclosures. It should also have provisions about how the contractor is to keep the information secure, and what it must do with the information when it has completed the contracted out activity (see paragraph 7.22.1).

**NPP4 - Data Security**

16.13.17 NPP 4 requires organisations to take reasonable steps to protect the personal information held from misuse and loss, and from unauthorised access modification, or disclosure. It would be advisable where the School contracts out a function or activity to have in the contract provisions to assist in complying with NPP 4.

16.13.18 A contractor that is not a small business and which collects personal information from the School would have obligations of its own under NPP 4 to keep the information secure.

**NPP5 - Openness**

16.13.19 To meet its obligations under NPP 5.2, where the School contracts out functions and activities involving personal information would generally need to be able to tell a person who asks:

   (a) where it discloses personal information to contractors
   (b) the purposes for which it discloses personal information to contractors
   (c) the names and types of organisations to which it contracts out functions and activities involving disclosure of personal information, and
   (d) the contractual measures it takes (in general terms) to protect such personal information.

16.13.20 The School might wish to include this information in its Privacy Policy. The contractor also has an obligation to comply with NPP 5, but how it meets its obligation could be agreed with the School as long as the rights of the individual are no diminished.
SECTION 16 (A): SCHOOL COUNSELLORS AND PRIVACY

From time to time issues arise in relation to the role of School Counsellors and their obligations to pupils, the schools at which pupils are enrolled and the parents of those pupils. Other issues arise relating to the operation of the Privacy Act in relation to the record of personal information which is collected by Counsellors. These notes address these issues in the context of the CEC Privacy Manual for Schools.

When reading these notes it is important to remember that:

(a) Counsellors do not enjoy any general “legal professional privilege”.

(b) Counsellors must respond to Summons and Subpoenas (subject to Protected Confidences provisions, as set out immediately below).

(c) Counsellors have to maintain the confidence of their clients in the context of an ethical (not just a legal) relationship.

(d) Protected Confidences in NSW:

Under the NSW Criminal Procedure Act 1986 (“the Act”), communications in confidence between counsellors and victims of sexual assault, referred to as “protected confidences”, are exempt from production under subpoena subject to certain exceptions. Specifically, the court can order the production of the material if satisfied of the following:

(i) the documents have substantial probative value, i.e. they will provide significant assistance in establishing particular facts.

(ii) other evidence of the protected confidence or the contents of the document is not available.

(iii) the public interest in disclosing the documents outweighs the public interest in keeping them confidential. In assessing the public interest of disclosing the documents, the court must take into account the likelihood and nature or extent of harm that would be caused to the alleged victim.

Also, the definition of counselling means that it is possible that communications between victims of sexual assault and school personnel, in addition to specialist counsellors, may be subject to the protected confidence provisions.

(Note: Protected Confidences provisions do not change statutory reporting requirements in relation to either DoCS or the Ombudsman).

Professional Associations

It is not correct to say that the Codes of various professional bodies override obligations that a school Counsellor may have as an employee of a school or any contractual obligations to which the Counsellor may be subject. Neither do they override the
provisions of the Privacy Act. Most Codes promulgated by professional associations
appear to recognise this in varying degrees.

Having said this, it is recognised that it is essential that Counsellors build a rapport with
pupils who they counsel, and failure to maintain a confidence can damage this. The same
principle applies to teachers. Often, necessary information can be conveyed to a person
(i.e. School Principal) who has a legal obligation to receive it without betraying a
confidence. However, there will be some occasions where it is necessary to directly pass
on material which relates to the well being of a pupil of the school.

In this context reference should also be made to Section 8 of the CEC Privacy
Manual which deals with “Use and Disclosure”.

Effect of Employment Status of Counsellors

Employee

Where a Counsellor is employed by a School any records of personal information
collected or made by the Counsellor will become records of the employer. The School
Principal is able to call for those records which directly pertain to a pupil of the school in
the same way as he or she may call for the records made by any other School employee
which relate to school matters. Those records may also be accessed by the pupil in
accordance with the provisions of the Privacy Act unless they fall into an exception
contained in the National Privacy Principles. The question of access is discussed at
section 12 of the Privacy Manual.

Contractors

Where a contractor provides counselling services to the school, whether directly or
through a third party agency, the question of who 'owns' any records will depend upon
the relationship between the parties. However, as schools from time to time will require
reports from the Counsellor about pupils it will be necessary for a 'collection notice' to
encompass this collection, thus relieving the contractor of the obligation to provide a
separate collection notice. It is suggested this notice could form part of the general
collection notice given by the school.

Thus the collection notice may include a paragraph to the effect:

'The School contracts with an external service provider [or name] to provide
counselling services for pupils. The Principal may require the Counsellor to
inform him or her or other teachers of any issues the Counsellor believes may
be necessary for the School to know for the well-being or development of the
pupil who is counselled or other pupils at the School.'

In addition to Privacy issues, from the standpoint of exercising its duty of care a School
may also wish to include a provision in its agreement (contract) with the Counsellor to
the following effect:

'The Principal may require you to provide him/her with the names of pupils to
whom you are providing counselling services. In providing counselling services
you must give detailed consideration as to whether the School may be able to
give assistance to the pupil or pupils concerned or take action to prevent harm to the pupil. If the School may be able to give assistance or take action you must provide the Principal with sufficient particulars to enable the Principal to consider the relevant issues."

Under the Privacy Act, records of the Counsellor may be able to be accessed by the pupil. Records held by the School which came from the Counsellor would be liable to be provided by the School to the pupil on request, subject of course to any exemptions contained in the National Privacy Principles as mentioned earlier. (See CEC Manual Section 8 “Use and Disclosure”)

Counsellors in Private Practice

Counsellors in private practice will generally be engaged by the parents of the child. In this case the relationship is between the child, the parents and the Counsellor. The school has no role to play except as requested by the Counsellor with the authority of the parents or pupil, or as requested by the parents.

Does it matter who referred the pupil to the Counsellor?

Generally, this makes no difference to the position set out above. However, it is likely that the person making the referral may seek a report from the Counsellor. Where the Counsellor is a private practitioner the consent of the pupil would be required before that report could be provided. Where the Counsellor is an employee of the School or a contractor to the School, the School would not need the consent of the pupil before providing a report to the parents, provided that it could be established that the report was a related secondary purpose (or directly related, if health information) to providing schooling to the pupil and disclosure would be reasonably expected. This expectation would be dealt with through the 'collection notice'. Even if this were not the case disclosure to the parent may be necessary for the School to fulfil its duty of care, as discussed below.

Duty of Care

It is important for Counsellors to be aware that they need to work in conjunction with teachers at the School as a team so that both the Counsellor and the School can properly meet their obligations in relation to their duty of care. Where a Counsellor who is an employee, (and possibly a contractor depending on the terms and conditions of the particular contractual arrangement) fails to pass on relevant information and the pupil suffers injury as a result, the School may be found to be vicariously liable for the activity of that Counsellor. If a pupil fails to achieve the academic standards he or she may otherwise have achieved, had the School been aware of relevant material, the School may be found to be in breach of its contract to provide schooling with due care and skill.

Failure by a Counsellor to consult with relevant School staff, therefore, may have serious consequences for the School.

The issue of Duty of Care is referred to in section 16.2 of the Manual. In the context of duty of care, it is important to remember that the personal information is the personal information of the student, regardless of the age of the student. It can only be disclosed to parents if:
• disclosure is for the primary purpose of collection or for a related secondary purpose which is reasonably expected; or

• it is necessary to fulfil the School's duty of care to the pupil.

However, on occasions, even though disclosure to parents may be permitted, *for example*, as a reasonably expected secondary purpose, the School Principal may decide not to do so because he/she has formed the view that disclosure may result in the child suffering harm.
17. THERE MAY ALSO BE OCCASIONS WHERE DISCLOSURE IS PROHIBITED BECAUSE OF THE SCHOOL'S OBLIGATION UNDER CHILD PROTECTION RELEVANT EXEMPTIONS

17.1 Employee Records

17.1.1 An act done, or practice engaged in, by an organisation that is or was an employer of an individual is exempt from the scope of the Privacy Act if the act or practice is directly related to:

(a) a current or former employment relationship between the employer and the individual, and

(b) an employee record held by the organisation relating to the individual.

17.1.2 An 'employee record' is defined broadly to be a record of personal information relating to the employment of an employee.

17.1.3 This 'employee records' exemption does not extend to prospective employees, contractors, consultants or volunteers. Further, in the Australian Capital Territory and Victoria, there is no exemption in relation to the collection, use and disclosure of an employee’s health records. If this applies to your School, see Part 4.

17.1.4 This is of particular importance in relation to related bodies corporate having access to employee records (for example via a database, or centralised HR facility) of employees of related bodies corporate. In such a case the body corporate who is not the employer of the individual to whom the records relate will be subject to the requirements of the Act in collecting, using, disclosing etc those employee records. Thus where one School in a group of separately incorporated related Schools retains employment information for the group, employees of the other Schools will be able to access (under NPP 6) personal information which relates to them because it is not collected by their employer.

17.1.5 Where personal information about an employee is given to an organisation, such as the AIS, in order to provide advice, issues may arise as to whether a collection notice should be given and whether the employee can gain access to that information.

17.1.6 Acts of employers who use employee information for commercial purposes outside the employment context will not be exempt from the operation of the Act.

17.1.7 Examples of employee records include health information about an employee and personal information about any or all of the following:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee

(c) the terms and conditions of employment of the employee

(d) the employee's personal and emergency contact details

(e) the employee's performance or conduct

(f) the employee's hours of employment

(g) the employee's salary or wages

(h) the employee's membership of a professional or trade association

(i) the employee's trade union membership
the employee's recreation, long service, sick, personal, maternity, paternity or other leave, and
the employee's taxation, banking or superannuation affairs.

17.1.8 Some practices in relation to employees could possibly fall outside the employee records exemption.

Example:
A record of a staff member's place of birth (collected via a 'Banking Information Form') might not be directly related to the employment relationship and therefore not within the 'employee records' exemption.

17.1.9 Whether or not information of this nature will be considered as being directly related to the employment relationship will be a question of fact to be decided in the context of each case. However, the School should bear in mind the consequences of having information which falls outside the employee records exemption.

17.1.10 Where a record of employee personal information falls outside the employee records exemption and is subject to the Privacy Act, then it is only that part of the record which falls outside the exemption that will be subject to the Act and not the whole record.

17.1.11 If employee records are given to related organisations, no collection notice need be given, but the employee exemption will not apply in the hands of that related organisation.

**Recommendation**

17.1.12 If employee records are disclosed to a third party, the School should be aware that it will not be an 'employee record' in the hands of that third party and a collection notice should be given by or on behalf of the third party.

17.1.13 If employee records are given to related organisations no collection notice need be given, but the employee exemption will not apply in the hands of that related organisation.

17.1.14 Where employee records are given to third parties to enable them to provide advice, an issue of access may arise. An exemption may arise if there are 'anticipated legal proceedings', if there is 'an investigation of anticipated legal proceedings', or providing access would have an 'unreasonable impact on the privacy of others'. However, in other circumstances it may be wise if the information is de-identified.

17.1.15 Information provided to a central Catholic Education Office by employees in different schools remains in the hands of the one employer. If it is disclosed to another Catholic Education Office, an issue may arise as to whether a collection notice should be given by that second office.

17.2 Transfers between related Schools

17.2.1 Section 13B of the Privacy Act permits organisations that are related companies to share personal information without having to comply with certain NPPs. However, there are some limitations to this exception. It is unlikely that there will be many Schools in this category.

17.2.2 The Guidelines indicate that the company that originally collects personal information from an individual must take reasonable steps under NPP 1.3(d) to tell the individual at the time of collection that it intends to disclose information about them to a related company.

17.2.3 Subject to the above paragraph, the effect of this exemption is that a company may disclose personal information other than sensitive information to a related company regardless of the provisions of the NPPs which would otherwise prevent the disclosure of that information.

17.2.4 A School which receives personal information from a related body corporate does **not** have to:
(a) issue a collection notice or otherwise inform the individual that it has collected the information; and
(b) show that the collection was necessary for one or more of its functions or activities.

17.2.5 However, a School which receives personal information from a related body corporate may only use the information is collects in that way:
(a) for the primary purpose of collection of the first collecting body corporate
(b) for a reasonably expected related secondary purpose of collection of the first collecting body corporate, or
(c) with the individual's consent.

17.2.6 This exemption does not apply in a number of circumstances, including where:
(a) the information is sensitive information
(b) the first collecting School is not an 'organisation', or
(c) the information disclosed by the first collecting School is disclosed pursuant to an exempt act or practice under the Privacy Act (e.g. under the 'employee records' exemption).
PART 4

18. HEALTH RECORDS LEGISLATION

18.1 State Specific Health Records Legislation: A Brief Overview

18.1.1 In addition to the Federal Privacy Act, there are State and Territory laws which separately regulate the collection, use, storage and handling of health records.

18.1.2 The relevant State and Territory legislation applies as follows:

(a) in New South Wales - Health Records and Information Privacy Act 2002 (which will commence to operate on a date that is yet to be proclaimed);

(b) in the Australian Capital Territory - Health Records (Privacy and Access) Act 1997; and

(c) in Victoria - Health Records Act 2000.

18.1.3 Health records in a school environment (whether these records relate to parents, students or employees) need to be treated carefully.

18.1.4 Health information is a sub-set of 'sensitive information' under the Federal Privacy Act. Accordingly, the collection, use and handling of health records is already subject to the Federal Privacy Act. On this basis, the information and guidance which is set out in this Manual above concerning the collection, use and handling of 'sensitive information' under the Federal Act should be applied in the case of health information.

18.1.5 The relevant State and Territory laws relating to health information simply impose additional requirements upon the collection, use and handling of health records and in some cases, limit the exemptions which otherwise apply under the Federal Privacy Act. These State and Territory laws apply in conjunction with the Federal Privacy Act, except where the State or Territory law is inconsistent with the Federal Privacy Act, in which case the Federal Privacy Act will prevail.

18.1.6 The health specific legislation in NSW, Victoria and the ACT is slightly different. On that basis, Schools based in Victoria, NSW and the ACT should independently check that they are complying with their specific obligations when dealing with health records.

18.1.7 Finally, it is recommended that if in doubt about specific obligations under the relevant State or Territory health records legislation or the application of the Federal Privacy Act to health records, then advice should be sought.

18.2 Health Privacy Principles

18.2.1 Each of the State and Territory Acts include a unique set of health privacy principles (each known as 'HPPs'), which operate in a similar way to the National Privacy Principles ('NPPs') and are broadly consistent with the NPPs.

(a) at Annexure D is a copy of the 15 HPPs which apply in New South Wales;

(b) at Annexure E is a copy of the 11 HPPs which apply in Victoria;

(c) at Annexure F is a copy of the 12 HPPs which apply in the Australian Capital Territory.

18.2.2 In broad terms, the HPPs supplement the NPPs and cover both public and private sector organisations.

18.2.3 In relation to schools, the State and Territory legislation broadly operates (subject to the
exemption in respect of employees in NSW) to:

(a) protect the privacy of an individual's 'health information' collected, used and held by that School;
(b) enable individuals to gain access to their health information held by the School; and
(c) provides an accessible framework to resolve complaints regarding the handling of health information by the School.

18.3 What is health information?

18.3.1 Health information generally includes personal information that is:

• information or opinion about a person's physical, mental health, or psychological health
• information or an opinion about an individual's express wishes about the future provision of health services to him or her
• information collected to provide, or in providing, a 'health service'
• information collected in relation to organ donation or genetic information.

18.4 Important Exemption in New South Wales

18.4.1 Importantly, in New South Wales, the definition of 'personal information' (which includes health information) expressly excludes 'employee records'. In this context, an 'employee records' takes its meaning from the Federal Privacy Act.

18.4.2 Accordingly, when using this Manual, schools in New South Wales should be aware that they are exempt from complying with the terms of the New South Wales Health Records and Information Privacy Act 2002 in respect of an employee's health records.

18.4.3 Note that this exemption does not extend to prospective employees and does not include contractors. The exemption does not apply in Victoria or the Australian Capital Territory.

18.4.4 Further, for a school in New South Wales to rely on this exemption, the relevant record must satisfy the requirements under the Federal Privacy Act about what constitutes an 'employee record'. As to these requirements, see chapter 2.6 above.

18.5 Complying with the HPPs

18.5.1 As set out above, the HPPs in each State and Territory are slightly different. There are, however, a number of broad principles which apply in each State and Territory. Some general guidance on how to comply with these principles is set out below.

18.5.2 It is suggested that in complying with the HPPs, the guidance set out in respect of the equivalent NPPs, particularly in relation to sensitive information, is reviewed and applied.

18.6 Particular Issues Relating to Health Information in Schools

18.6.1 There are special issues which arise in a school environment and would have an impact on how a school is able to collect, use and handle health records - particularly those records relating to students.

18.6.2 At Chapter 16 above, there are a range of particular schools issues raised and guidance about how to deal with those issues. The guidance set out in Chapter 16 above would broadly apply to the collection, use and handling of health records under the relevant State and Territory legislation.

18.6.3 Set out below are some additional issues which may arise in the context of collecting, using and handling health records.
18.7 Collection

18.7.1 Schools should ensure that health information collected is necessary for one or more of the school’s functions. For example:

(a) health information about a teacher should generally only be collected where that information is necessary for the purpose of employment records or to enable the School to make an assessment about whether a teacher is able to perform their job properly, safely and compliance with all laws and obligations (note that this obligation only applies in Victoria and the Australian Capital Territory due to the employee records exemption in other States and Territories);

(b) health information about a student should only be collected where it is necessary for the school to provide services and adequate care for that student or to protect others in the school environment. In this regard, it is important to ensure that the collection of this information is not undertaken in an unreasonably intrusive way.

18.7.2 The HPPs generally require that information is collected from the individual directly, unless it is unreasonable or impracticable to do so. In some circumstances, it will be impracticable to collect health information directly from the individual concerned. This may arise particularly in relation to the collection of health information about students, but does not necessarily arise in relation to the collection of information about teachers and other adults working or associated with the school community.

18.8 Storage

18.8.1 Like all personal information, health information should be stored in a secure place, protected from unauthorised access and not kept any longer than necessary. However, the HPPs impose certain additional storage requirements - see paragraph 18.11.6 below.

18.8.2 Once the health information is no longer necessary, the information should be confidentially destroyed.

18.9 Access and Accuracy

18.9.1 An individual should be aware that health information about them has been collected and is being stored and that they have a right to access that information.

18.9.2 Note that there are a range of grounds on which access need not be granted. These grounds are generally similar to the grounds on which a school may refuse access to personal information (see Chapter 12 above). It is suggested that this part of the Manual is reviewed if a request for access is made.

18.9.3 Individuals have a right to request that a school amend their health information to ensure that it is accurate, up to date and, having regard to purpose for which it was collected, is relevant. If a school is unwilling to correct or amend an individual's record, then the school is required to attach a statement to that individual's file or records which documents the individual's request that their records be amended.

18.10 Disclosure and Use

18.10.1 There are limitations on how health information may be used and disclosed. These limitations are broadly similar to those limitations which apply to sensitive information under the Federal Privacy Act (see Chapter 7 above).

18.11 Schools as 'Health Service Provider'

18.11.1 The provision of a 'health service' by a School to a student does not necessarily make that School a 'health service provider' subject to the health records legislation.

18.11.2 However, in some instances, a School could be found to be a 'health service provider' and as
a result, may have some additional obligations in relations to the records it collects in the course of providing that service.

18.11.3 By way of example, those Schools which provide:
   (a) an in-house nursing and/or medical service;
   (b) an in-house psychologist/counsellor; or
   (c) an in-house speech pathologist,
could, depending on the circumstances, be found to be a 'health service provider'.

18.11.4 Where a School includes general 'health issues' in its syllabus, an argument may arise that it is a 'health service provider' on the basis that 'health service' is defined in the health records legislation to include the provision of 'health education services'. However, it is not likely that this would be found to be the case.

18.11.5 For those schools which are found to be 'health service providers' under the health records legislation, it is important to remember that the provision of these services are already regulated by the Federal Privacy Act (see a School's obligations regarding the collection of 'sensitive information' at Chapter 7 above).

18.11.6 The health records legislation imposes certain additional obligations on 'health service providers' than otherwise imposed by the Federal Privacy Act. For example, in New South Wales and Victoria, the information must be retained:
   (a) for 7 years (in the case of collection from individuals over 18) or;
   (b) where collection is from a child under 18, until that child reaches 25, and to make certain records where that information is disclosed or divested.

18.11.7 Where a School employs such a in-house professional to provide a health service (eg psychologist or speech therapist), Schools assume the record keeping responsibility for the services that the professional provides through his or her employment with the School.

18.11.8 In house professional employees should not be permitted to hold on to their own health records to the exclusion of the School, as this may impede the School's ability to comply with its obligations under the health records legislation. Further, employees should not be permitted to take records with them if they cease employment with the School, as again, this would cause difficulties for Schools in complying with its record-keeping obligations under the health records legislation.
19. ANNEXURE A - PRIVACY POLICY

19.1 A Privacy Policy is needed to inform individuals about the practices of the School in relation to personal information. It also serves as a guide to the School's staff as to the standards to be applied in respect of handling personal information and ensure consistency in the School's approach to privacy.

19.1.1 The following draft Privacy Policies are intended to allow the School to satisfy the requirements of NPP 5, dealing with openness.

19.1.2 There are two draft Privacy Policies annexed. The first is appropriate for non systemic Schools and the latter is appropriate for systems and Schools operating within systems.

19.1.3 The Policy which the School adopts may be used, in conjunction with the collection notices, to satisfy the requirements in NPPs 1.3 and 1.5 to ensure that individuals are aware of relevant matters on collection of personal information.

19.1.4 The policies are drafts only and must be adapted to each School or system's particular acts and practices.
Draft Privacy Policy

Your privacy is important

This statement outlines the Schools' policy on how the School uses and manages personal information provided to or collected by it.

The School is bound by the National Privacy Principles contained in the Commonwealth Privacy Act. In relation to health records, the School is also bound by the New South Wales Health Privacy Principles which are contained in the Health Records and Information Privacy Act 2002 (Health Records Act).

The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School’s operations and practices and to make sure it remains appropriate to the changing school environment.

What kind of personal information does the School collect and how does the School collect it?

The type of information the School collects and holds includes (but is not limited to) personal information, including sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School;
- job applicants, staff members, volunteers and contractors; and
- other people who come into contact with the School.

Personal Information you provide: The School will generally collect personal information held about an individual by way of forms filled out by Parents or pupils, face-to-face meetings and interviews, and telephone calls. On occasions people other than Parents and pupils provide personal information.

Personal Information provided by other people: In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

Exception in relation to employee records: Under the Privacy Act and the Health Records Act the National Privacy Principles and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and employee.

How will the School use the personal information you provide?

The School will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

Pupils and Parents: In relation to personal information of pupils and Parents, the School's primary purpose of collection is to enable the School to provide schooling for the pupil. This
includes satisfying both the needs of Parents and the needs of the pupil throughout the whole period the pupil is enrolled at the School.

The purposes for which the School uses personal information of pupils and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration;
- looking after pupils' educational, social and medical wellbeing;
- seeking donations and marketing for the School;
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

In some cases where the School requests personal information about a pupil or Parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the pupil.

Job applicants, staff members and contractors: In relation to personal information of job applicants, staff members and contractors, the School's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

The purposes for which the School uses personal information of job applicants, staff members and contractors include:

- in administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the School;
- to satisfy the School's legal obligations, for example, in relation to child protection legislation.

Volunteers: The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as [alumni associations], to enable the School and the volunteers to work together.

Marketing and fundraising: The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to be a quality learning environment in which both pupils and staff thrive. Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising, for example, the School's Foundation or alumni organisation.

Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

Who might the School disclose personal information to?

The School may disclose personal information, including sensitive information, held about an individual to:

- another school;
- government departments;
- medical practitioners;
• people providing services to the School, including specialist visiting teachers, counsellors and sports coaches;
• recipients of School publications, like newsletters and magazines;
• Parents;
• anyone you authorise the School to disclose information to; and
• anyone to whom we are required to disclose the information to by law.

Sending information overseas: The School will not send personal information about an individual outside Australia without:

• obtaining the consent of the individual (in some cases this consent will be implied); or
• otherwise complying with the National Privacy Principles or other applicable privacy legislation.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record, that is also personal information; and health information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

The School's staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals.

The School has in place steps to protect the personal information the School holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and pass worded access rights to computerised records.

Updating personal information

The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by the School by contacting the [Secretary] of the School at any time.

The National Privacy Principles and the Health Privacy Principles require the School not to store personal information longer than necessary. In particular, the Health Privacy Principles impose certain obligations about the length of time health records must be stored.

You have the right to check what personal information the School holds about you

Under the Commonwealth Privacy Act and the Health Records and Information Privacy Act, an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. There are some exceptions to
this right set out in the applicable legislation. Pupils will generally have access to their personal information through their Parents, but older pupils may seek access themselves. To make a request to access any information the School holds about you or your child, please contact the School Principal in writing.

The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Consent and rights of access to the personal information of pupils

The School respects every Parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's Parents. The School will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.

Parents may seek access to personal information held by the School about them or their child by contacting the [School Principal]. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the pupil.

The School may, at its discretion, on the request of a pupil grant that pupil access to information held by the School about them, or allow a pupil to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances so warranted.

You may seek access to the personal information the School holds about you

Under the Commonwealth Privacy Act and the Health Records Act, an individual may seek access to personal information which the School holds about them. There are some exceptions to this set out in the applicable legislation. Pupils will generally have access to their personal information through their Parents, but older pupils may seek access themselves.

To make a request to access any information the School holds about you or your child, please contact the School Principal in writing.

The School may require you to verify your identity and specify what information you require. The School may charge a fee for access and will advise the likely cost in advance.

Enquiries

If you would like further information about the way the School manages the personal information it holds, please contact the [School Principal].
Draft Privacy Policy

[Catholic Education Office of the […] Diocese / …System]

Your privacy is important

This Privacy Policy applies to schools conducted by the [Catholic Education Office of the […] Diocese (the 'CEO') / System].

This statement outlines the [CEO's / System's] policy on how each school uses and manages personal information provided to or collected by it.

The [CEO / System] is bound by the National Privacy Principles contained in the Commonwealth Privacy Act. In relation to health records the [CEO / System] is also bound by the Health Privacy Principles contained in the Health Records and Information Privacy Act 2002 (Health Records Act).

The [CEO / System] may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to schools' operations and practices and to make sure it remains appropriate to the changing school environment.

What kind of personal information does a school collect and how does a school collect it?

The type of information schools collect and hold includes (but is not limited to) personal information, including sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the school;
- job applicants, staff members, volunteers and contractors; and
- other people who come into contact with the school.

Personal Information you provide: A school will generally collect personal information held about an individual by way of forms filled out by Parents or pupils, face-to-face meetings and interviews, and telephone calls. On occasions people other than Parents and pupils provide personal information.

Personal Information provided by other people: In some circumstances a school may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

Exception in relation to employee records: Under the Privacy Act and the Health Records Act the National Privacy Principles and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the school and employee.
How will a school use the personal information you provide?

A school will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

Pupils and Parents: In relation to personal information of pupils and Parents, a school's primary purpose of collection is to enable the school to provide schooling for the pupil. This includes satisfying both the needs of Parents and the needs of the pupil throughout the whole period the pupil is enrolled at the school.

The purposes for which a school uses personal information of pupils and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration;
- looking after pupils' educational, social, spiritual and medical wellbeing;
- seeking donations and marketing for the school;
- to satisfy the [CEO's / System's] and the school's legal obligations and allow the school to discharge its duty of care.

In some cases where a school requests personal information about a pupil or Parent, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the pupil.

Job applicants, staff members and contractors: In relation to personal information of job applicants, staff members and contractors, a school's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

The purposes for which a school uses personal information of job applicants, staff members and contractors include:

- in administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the school;
- to satisfy the [CEO's / System's] and the school's legal obligations, for example, in relation to child protection legislation.

Volunteers: A school also obtains personal information about volunteers who assist the school in its functions or conduct associated activities, such as [alumni associations], to enable the school and the volunteers to work together.

Marketing and fundraising: Schools treat marketing and seeking donations for the future growth and development of the school as an important part of ensuring that the school continues to be a quality learning environment in which both pupils and staff thrive. Personal information held by a school may be disclosed to an organisation that assists in the school's fundraising, for example, the school's Foundation or alumni organisation.

Parents, staff, contractors and other members of the wider school community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.
**Exception in relation to related schools:** The Privacy Act allows each school, being legally related to each of the other schools conducted by the [CEO / System] to share personal (but not sensitive) information with other schools conducted by the [CEO / System]. Other [CEO / System], schools may then only use this personal information for the purpose for which it was originally collected by the [CEO / System]. This allows schools to transfer information between them, for example, when a pupil transfers from a [CEO / System] school to another school conducted by the [CEO / System].

**Who might a school disclose personal information to?**

A school may disclose personal information, including sensitive information, held about an individual to:

- another school;
- government departments;
- your local parish;
- medical practitioners;
- people providing services to the school, including specialist visiting teachers, counsellors and sports coaches;
- recipients of school publications, like newsletters and magazines;
- Parents;
- anyone you authorise the school to disclose information to; and
- anyone to whom we are required to disclose the information by law.

**Sending information overseas:** A school will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the National Privacy Principles or other applicable privacy legislation.

**How does a school treat sensitive information?**

In referring to 'sensitive information', a school means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record, that is also personal information; and health information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

**Management and security of personal information**

The [CEO's / System's] and the schools' staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals.

Each school has in place steps to protect the personal information the school holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and pass worded access rights to computerised records.
Updating personal information

Each school endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by a school by contacting the [Secretary] of the school at any time.

The National Privacy Principles require a school not to store personal information longer than necessary. The Health Records Act requires health records to be stored for a particular period depending on the age of the individual.

You have the right to check what personal information a school holds about you

Under the Commonwealth Privacy Act and Health Records Act, an individual has the right to obtain access to any personal information which the [CEO / System] or a school holds about them and to advise the [CEO / System] or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Pupils will generally have access to their personal information through their Parents, but older pupils may seek access themselves.

To make a request to access any information the [CEO / System] or a school holds about you or your child, please contact the school's Principal in writing.

The school may require you to verify your identity and specify what information you require. The school may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the school will advise the likely cost in advance.

Consent and rights of access to the personal information of pupils

The [CEO / System] respects every Parent's right to make decisions concerning their child's education.

Generally, a school will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's Parents. A school will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.

Parents may seek access to personal information held by a school or the [CEO / System] about them or their child by contacting the [school's Principal]. However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the pupil.

A school may, at its discretion, on the request of a pupil grant that pupil access to information held by the school about them, or allow a pupil to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances so warranted.

You may seek access to the personal information the School holds about you

Under the Commonwealth Privacy Act and Health Records Act, an individual may seek access to personal information which the School holds about them. There are some exceptions to this
set out in the applicable legislation. Pupils will generally have access to their personal information through their Parents, but older pupils may seek access themselves. To make a request to access any information the School holds about you or your child, please contact the School Principal in writing.

The School may require you to verify your identity and specify what information you require. The School may charge a fee for access and will advise the likely cost in advance.

**Enquiries**

If you would like further information about the way the [CEO / System] or a school manages the personal information it holds, please contact the [school's Principal].
20. ANNEXURE B - EMAIL AND INTERNET POLICY

20.1 Personal information may be collected, used, disclosed, stored and transferred overseas through the use of email and Internet facilities.

20.1.1 The following Email and Internet Policy takes into account the requirements of the Privacy Act. Schools may already have email policies which could be adapted to meet the requirements of the Privacy Act.

20.1.2 In addition, the School should adopt a Privacy Policy for its website where relevant. The Privacy Commissioner has issued a guide for Federal and ACT Government website privacy policies. The School should consider whether the guide, or aspects of it, would be relevant for the School. The guide is located on the Privacy Commissioner's website at: http://www.privacy.gov.au/internet/index.html
This document sets out the security, administration and internal rules which you should observe when communicating electronically or using the IT facilities provided by [insert name of school] (the 'School'). You should familiarise yourself with the terms of this Policy in order to minimise potential damage to you, your colleagues, students and the School, which may arise as a result of misuse of email or Internet facilities.

This Policy applies to all teachers, employees and contractors of the School.

1. **School Property**

   1.1 The School is the owner of copyright in all email messages created by its employees and contractors in performing their duties.

2. **Monitoring**

   2.1 The contents and usage of email may be examined by the School or by a third party on the School's behalf. This will include electronic communications which are sent to you or by you, both internally or externally. You should expect this monitoring to be continuous and ongoing.

   2.2 You should structure your email in recognition of the fact that the School may examine its contents.

   2.3 The School's computer network is a business and educational tool to be used primarily for business or educational purposes. You therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.

   2.4 All messages on the School's system will be treated as education or business related messages, which may be monitored. Accordingly, you should not expect that any information or document transmitted or stored on the School's computer network will be private.

   2.5 You should also be aware that the School is able to monitor your use of the Internet, both during school or working hours and outside of those hours. This includes the sites and content that you visit and the length of time you spend using the Internet.

   2.6 The School may block access to certain websites and/or delivery of certain emails as it considers appropriate.

   2.7 Emails will be archived by the School as it considers appropriate.

   2.8 The School may copy, access or disclose any information or files that are stored, processed or transmitted using the School's computer network.
3. Personal Use

3.1 You are permitted to use the Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the performance of your work duties.

3.2 However, you should bear in mind that any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.

3.3 In the case of shared IT facilities, you are expected to respect the needs of your colleagues and use the Internet and email in a timely and efficient manner.

3.4 Excessive or inappropriate use of email or Internet facilities for personal reasons during working hours may lead to disciplinary action.

4. Content

4.1 Email correspondence should be treated in the same way as any other correspondence, such as a letter or a fax. That is, as a permanent written record which may be read by persons other than the addressee and which could result in personal or the School's liability.

4.2 You and/or the School may be liable for what you say in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

4.3 You should never use the Internet or email for the following purposes:

   (a) to abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other);
   (b) to send or receive obscene or pornographic material;
   (c) to injure the reputation of the School or in a manner that may cause embarrassment to your employer;
   (d) to spam or mass mail or to send or receive chain mail;
   (e) to infringe the copyright or other intellectual property rights of another person; or
   (f) to perform any other unlawful or inappropriate act.

4.4 Email content that may seem harmless to you may in fact be highly offensive to someone else. You should be aware, therefore, that in determining whether an email falls within any of the categories listed above, or is generally inappropriate, the School will consider the response and sensitivities of the recipient of an email rather than the intention of the sender.

4.5 If you receive inappropriate material by email, you should delete it immediately and not forward it to anyone else. It would be appropriate for you to discourage the sender from sending further materials of that nature.

4.6 Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by email. Email messages can easily be misconstrued.
Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

4.7 You should be aware that use of the School's computer network in a manner inconsistent with this policy or in any other inappropriate manner, including but not limited to use for the purposes referred to in paragraph 4.3 of this policy, will give rise to disciplinary action, including termination of an employee's employment or contractor's engagement.

5. **Privacy**

5.1 In the course of carrying out your duties on behalf of the School, you may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another except in accordance with the School's Privacy Policy or with proper authorisation.

5.2 The Privacy Act requires both you and the School to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. We stress therefore, that you take responsibility for the security of your personal computer and not allow it to be used by an unauthorised party, which specifically includes anyone who is not an employee of the School.

5.3 You will be assigned a log-in code and you will also select a password to use the School's electronic communications facilities. You should ensure that these details are not disclosed to anyone else. We suggest that you take steps to keep these details secure. For example, you should change your password regularly and ensure that your log-in code and password are not kept in writing close to your working area.

5.4 You are encouraged to either lock your screen or log-out when you leave your desk. This will avoid others gaining unauthorised access to your personal information, the personal information of others and confidential information within the School.

5.5 In order to comply with the School's obligations under the Privacy Act, you are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.

5.6 In addition to the above, you should familiarise yourself with the National Privacy Principles ('NPPs') and ensure that your use of email does not breach the Privacy Act or the NPPs. If you require more information on the Privacy Act and how to comply, please contact [the School Principal].

6. **Distribution and Copyright**

6.1 When distributing information over the School's computer network or to third parties outside the School, you must ensure that you and the School have the right to do so, and that you are not violating the intellectual property rights of any third party.

6.2 If you are unsure of whether you have sufficient authorisation to distribute the information, we recommend that you contact [responsible School officer].

6.3 In particular, copyright law may apply to the information you intend to distribute and must always be observed. The copyright material of third parties (for example, software,
database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so.

7. **Encryption and Confidentiality**

7.1 When email is sent from the School to the network server and then on to the Internet, the email message may become public information. Encryption will reduce the risk of third parties being able to read email and should be used in cases where you feel additional security is required. If you require more information in relation to encrypting messages, you should contact [the IT department].

7.2 As mentioned above, the Internet and email are insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent via email. You should note that there is always a trail and a copy saved somewhere, not necessarily only on the School's network server.

7.3 This confidentiality requirement applies even when encryption is used.

7.4 Email sent over the Internet may be truncated, scrambled, or sent to the wrong address. There is a possibility that outgoing email sent over the Internet may arrive scrambled or truncated, may be delayed, may not arrive at all, or may be sent to the wrong address. Where outgoing email is important or urgent, you should verify that the recipient has received the email in its entirety.

7.5 You must ensure that all emails that are sent from your email address contain the School's standard disclaimer message, which will read as follows:

   *The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please advise by telephone (reverse charges) immediately and then delete/destroy the email and any printed copies. Thankyou.*

   [This message will be set to appear automatically on each outgoing email. Please contract IT if this feature is not working]

7.6 There is a risk of false attribution of email. Software is widely available by which email messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender of incoming email. You should verify the identity of the sender by other means if you have concerns.

7.7 Please delete old or unnecessary email messages and archive only those email messages you need to keep. Retention of messages fills up large amounts of storage space on the network server and can slow down performance. You should maintain as few messages as possible in your in-boxes and out-boxes. If there are items in your email which you require at later date, please ensure that these are saved in your network directory so that appropriate backups are made School wide.
8. **Viruses**

8.1 All external files and attachments must be virus checked using scanning software before they are accessed. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the School computer network.

8.2 A document attached to an incoming email may have an embedded virus.

8.3 Virus checking is done automatically through the [*virus protector software*] installed on the [*network server*] and [*any other virus protective action*?]. If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact [*IT department*].

9. **Absence**

9.1 In cases where you are likely to be absent from work for any period of time, you should make arrangements for your emails to be accessible by the School or ensure that an 'out of office reply' is automatically set. This automatic reply will alert those trying to contact you that you are away from work and that important queries should be directed to a nominated colleague. If you require assistance in installing this feature, please contact [*IT department*].

10. **Policy Updates**

10.1 This policy may be updated or revised from time to time. The School will not notify you each time the Policy is changed. If you are unsure whether you are reading the most current version, you should contact [*School Principal / or review the latest School policies on the School's intranet*?].

11. **General**

11.1 The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the Internet, you should contact [*School Principal*].
21. ANNEXURE C - NATIONAL PRIVACY PRINCIPLES

21.1 Annexure C is the full text of the NPPs as contained in Schedule 3 to the Privacy Act. The NPPs and the Privacy Act are contained on the Privacy Commissioner's website:

http://www.privacy.gov.au/publications/npps01.html#a
ANNEXURE C:

1. **Collection**

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

   (a) the identity of the organisation and how to contact it; and
   (b) the fact that he or she is able to gain access to the information; and
   (c) the purposes for which the information is collected; and
   (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
   (e) any law that requires the particular information to be collected; and
   (f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. **Use and disclosure**

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

   (a) both of the following apply:
      (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
      (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
   (b) the individual has consented to the use or disclosure; or
(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure - the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation or the matter or in reporting its concerns to relevant persons or authorities; or
(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment or criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

   (i) is physically or legally incapable of giving consent to the disclosure; or

   (ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the carer) providing the health service for the organisation is satisfied that either:
(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is 'responsible' for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

'child' of an individual includes an adopted child, a step-child and a foster-child, of the individual.

'parent' of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

'relative' of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

'sibling' of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3. Data Quality
An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4. **Data Security**

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5. **Openness**

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. **Access and correction**

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

   (a) in the case of personal information other than health information - providing access would pose a serious and imminent threat to the life or health of any individual; or

   (b) in the case of health information - providing access would pose a serious threat to the life or health of any individual; or

   (c) providing access would have an unreasonable impact upon the privacy of other individuals; or

   (d) the request for access is frivolous or vexatious; or

   (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

   (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

   (g) providing access would be unlawful; or

   (h) denying access is required or authorised by or under law; or
(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.
6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7. **Identifiers**

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

'identifier' includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an 'identifier'.

8. **Anonymity**

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.
9. Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10. Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or
(d) if the information is collected in the course of the activities of a non-profit organisation - the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or
(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

'non-profit organisation' means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims.
22. ANNEXURE D - HEALTH PRIVACY PRINCIPLES - NEW SOUTH WALES

Annexure D is the full text of the HPPs as contained in Schedule 1 to the Health Records and Information Privacy Act 2002. The HPPs and the Health Records and Information Privacy Act 2002 are available on the Privacy Commissioner's website under the section titled Australian State Government links:

The full text of the NSW HPPs are attached.
ANNEXURE D:

Principle 1 - Purposes of collection of health information

1. An organisation must not collect health information unless:
   (a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and
   (b) the collection of the information is reasonably necessary for that purpose.

2. An organisation must not collect health information by any unlawful means.

Principle 2 - Information must be relevant, not excessive, accurate and not intrusive

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

   (a) the information collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and
   (b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Principle 3 - Collection to be from individual concerned

1. An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

2. Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

Principle 4 - Individual to be made aware of certain matters

1. An organisation that collects health information about an individual from the individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:

   (a) the identity of the organisation and how to contact it,
   (b) the fact that the individual is able to request access to the information,
   (c) the purposes for which the information is collected,
   (d) the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind,
   (e) any law that requires the particular information to be collected,
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

2. If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that:

(a) making the individual aware of the matters would pose a serious threat to the life or health of any individual, or

(b) the collection is made in accordance with guidelines issued under subclause (3).

3. The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

4. An organisation is not required to comply with a requirement of this clause if:

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it, or

(b) the organisation is lawfully authorised or required not to comply with it, or

(c) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or

(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or

(e) the information concerned is collected for law enforcement purposes, or

(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

5. If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances to ensure that any authorised representative of the individual is aware of those matters.

6. Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

7. The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

**Principle 5 - Retention and security**

1. An organisation that holds health information must ensure that:
(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and

(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of the organisation is done to prevent unauthorised use or disclosure of the information.

Note: Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

2. An organisation is not required to comply with a requirement of this clause if:

    a) the organisation is lawfully authorised or required not to comply with it, or
    b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

3. An investigative agency is not required to comply with subclause (1) (a).

Principle 6 - Information about health information held by organisations

1. An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain:

    a) whether the organisation holds health information, and
    b) whether the organisation holds health information relating to that individual, and
    c) if the organisation holds health information relating to that individual:

        (i) the nature of that information, and
        (ii) the main purposes for which the information is used, and
        (iii) that person’s entitlement to request access to the information.

2. An organisation is not required to comply with a provision of this clause if:

    a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
    b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).
Principle 7 - Access to health information

1. An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

   **Note:** Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Access to health information held by public sector agencies may also be available under the Freedom of Information Act 1989 or the State Records Act 1998.

2. An organisation is not required to comply with a provision of this clause if:
   
   (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

   (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

Principle 8 - Amendment of health information

1. An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:

   (a) is accurate, and

   (b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

2. If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

3. If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.

   **Note:** Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Amendment of health information held by public sector agencies may also be able to be sought under the Freedom of Information Act 1989.

4. An organisation is not required to comply with a provision of this clause if:

   (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

Principle 9 - Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

Principle 10 - Limits on use of health information

1. An organisation that holds health information must not use the information for a purpose (a "secondary purpose") other than the purpose (the "primary purpose") for which it was collected unless:

(a) Consent
the individual to whom the information relates has consented to the use of the information for that secondary purpose, or

(b) Direct relation
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or

Note: For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) Serious threat to health or welfare
the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(d) Management of health services
the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and
(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) Training
the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) Research
the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) Find Missing Person
the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or
(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**

the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a health registration Act, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(i) **Law enforcement**

the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(j) **Investigative agencies**

the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(k) **Prescribed circumstances**

the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

2. An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

3. The Ombudsman’s Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

4. Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

5. The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Principle 11 - Limits on disclosure of health information

1. An organisation that holds health information must not disclose the information for a purpose (a "secondary purpose") other than the purpose (the "primary purpose") for which it was collected unless:

   (a) **Consent**
     the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

   (b) **Direct relation**
     the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or

   **Note:** For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

   (c) **Serious threat to health or welfare**
     the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

     (i) a serious and imminent threat to the life, health or safety of the individual or another person, or

     (ii) a serious threat to public health or public safety, or

   (d) **Management of health services**
     the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

     (i) either:

       (A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or
(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training**

the disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research**

the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual’s identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual’s identity can reasonably be ascertained, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or
(g) **Compassionate reasons**
the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and

(ii) the individual is incapable of giving consent to the disclosure of the information, and

(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and

(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

(h) **Find missing person**
the disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(i) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline**
the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a health registration Act, or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement**
the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(k) **Investigative agencies**
the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(l) **Prescribed circumstances**

the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

2. An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(c) the organisation is an investigative agency disclosing information to another investigative agency.

3. The Ombudsman’s Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

4. Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

5. If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

6. The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

**Principle 12 - Identifiers**

1. An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

2. Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector
agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the individual has consented to the adoption of the same identifier, or
(b) the use or disclosure of the identifier is required or authorised by or under law.

3. Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)–(k) or 11 (1) (c)–(l), or
(b) the individual has consented to the use or disclosure, or
(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

4. If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or
(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

Principle 13 - Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

Principle 14 - Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or
(b) the individual consents to the transfer, or
(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual’s request, or
(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or

(e) all of the following apply:
   (i) the transfer is for the benefit of the individual,
   (ii) it is impracticable to obtain the consent of the individual to that transfer,
   (iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:
   (i) a serious and imminent threat to the life, health or safety of the individual or another person, or
   (ii) a serious threat to public health or public safety, or

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or

(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

Principle 15 - Linkage of health records

1. An organisation must not:

   (a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or

   (b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

2. An organisation is not required to comply with a provision of this clause if:

   (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

   (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or

   (c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

3. In this clause:
'health record' means an ongoing record of health care for an individual.

'health records linkage system' means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.
Annexure E is the full text of the HPPs as contained in Schedule 1 to the *Health Records Act 2001*. The HPPs and the *Health Records Act 2001* are available on the Privacy Commissioner's website under the section titled Australian State Government links:


The full text of the Victorian HPPs are attached.
ANNEXURE E:

1. **Principle 1 - Collection**

*When health information may be collected*

1.1 An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies:

(a) the individual has consented;

(b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law);

(c) the information is necessary to provide a health service to the individual and the individual is incapable of giving consent within the meaning of section 85(3) and:

(i) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(ii) the individual does not have such an authorised representative;

(d) the information is disclosed to the organisation in accordance with HPP 2.2(a), (f), (i) or (l) or HPP 2.5;

(e) if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest:

(i) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(ii) it is impracticable for the organisation to seek the individual's consent to the collection; and

(iii) the information is collected in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph;

(f) the collection is necessary to prevent or lessen:

(i) a serious and imminent threat to the life, health, safety or welfare of any individual; or

(ii) a serious threat to public health, public safety or public welfare

and the information is collected in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph;
(g) the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for a law enforcement function;

(h) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(i) the collection is in the prescribed circumstances.

How health information is to be collected

1.2 An organisation must collect health information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 If it is reasonable and practicable to do so, an organisation must collect health information about an individual only from that individual.

1.4 At or before the time (or, if that is not practicable, as soon as practicable thereafter) an organisation collects health information about an individual from the individual, the organisation must take steps that are reasonable in the circumstances to ensure that the individual is generally aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.5 If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is or has been made aware of the matters listed in HPP 1.4 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual or would involve the disclosure of information given in confidence.

1.6 An organisation is not required to notify the individual of the identity of persons, or classes of persons, to whom health information may be disclosed in accordance with HPP 2.2(f).

Information given in confidence

1.7 If personal information is given in confidence to a health service provider about an individual by a person other than:
(a) the individual; or
(b) a health service provider in the course of, or otherwise in relation to, the provision of health services to the individual

with a request that the information not be communicated to the individual to whom it relates, the provider must:

(c) confirm with the person that the information is to remain confidential; and
(d) if the information remains confidential:
   (i) record the information only if it is relevant to the provision of health services to, or the care of, the individual; and
   (ii) take reasonable steps to ensure that the information is accurate and not misleading; and
(e) take reasonable steps to record that the information is given in confidence and is to remain confidential.

2. **Principle 2 - Use and Disclosure**

2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1.

2.2 An organisation must not use or disclose health information about an individual for a purpose (the "secondary purpose") other than the primary purpose for which the information was collected unless at least one of the following paragraphs applies:

(a) both of the following apply:
   (i) the secondary purpose is directly related to the primary purpose; and
   (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
(b) the individual has consented to the use or disclosure; or
(c) the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law); or
(d) all of the following apply:
   (i) the organisation is a health service provider providing a health service to the individual; and
   (ii) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and
   (iii) the individual is incapable of giving consent within the meaning of section 85(3) and:
(A) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(B) the individual does not have such an authorised representative; or

(e) all of the following apply:

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and

(iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and

(iv) the information is used in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(f) the use or disclosure is for the purpose of:

(i) funding, management, planning, monitoring, improvement or evaluation of health services; or

(ii) training provided by a health service provider to employees or persons working with the organisation; and

(iii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the individual's consent to the use or disclosure; or

(iv) reasonable steps are taken to de-identify the information; and

(v) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(vi) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph; or

(g) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
(ii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(iii) the use or disclosure is in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph; and

(iv) in the case of disclosure:

(A) the organisation reasonably believes that the recipient of the health information will not disclose the health information; and

(B) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; or

(h) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety or public welfare

and the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(i) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(j) the organisation reasonably believes that the use or disclosure is reasonably necessary for a law enforcement function by or on behalf of a law enforcement agency and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(k) the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(l) the use or disclosure is in the prescribed circumstances.

Note: Nothing in HPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.

2.3 If an organisation discloses health information under paragraph (i) or (j) of HPP 2.2, it must make a written note of the disclosure.
2.4 Despite HPP 2.2, a health service provider may disclose health information about an individual to an immediate family member of the individual if:

(a) either:

(i) the disclosure is necessary to provide appropriate health services to or care of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(b) the disclosure is limited to the extent reasonable and necessary for the purposes mentioned in paragraph (a); and

(c) the individual is incapable of giving consent to the disclosure within the meaning of section 85(3); and

(d) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then; and

(ii) of which the organisation is aware or could be made aware by taking reasonable steps; and

(e) in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.

2.5 Despite HPP 2.2, an organisation may use or disclose health information about an individual where:

(a) it is known or suspected that the individual is dead; or

(b) it is known or suspected that the individual is missing; or

(c) the individual has been involved in an accident or other misadventure and is incapable of consenting to the use or disclosure

and the use or disclosure is to the extent reasonably necessary;

(d) to identify the individual; or

(e) to ascertain the identity and location of an immediate family member or other relative of the individual for the purpose of:

(i) enabling a member of the police force, a coroner or other prescribed organisation to contact the immediate family member or other relative for compassionate reasons; or

(ii) to assist in the identification of the individual
and, in the circumstances referred to in paragraph (b) or (c);

(f) the use or disclosure is not contrary to any wish:

   (i) expressed by the individual before he or she went missing or became
       incapable of consenting and not withdrawn by the individual; and

   (ii) of which the organisation is aware or could have become aware by taking
       reasonable steps; and

(g) the information is used or disclosed in accordance with guidelines, if any, issued
    or approved by the Health Services Commissioner under section 22 for the
    purposes of this paragraph.

3. Principle 3 - Data Quality

3.1 An organisation must take steps that are reasonable in the circumstances to make sure
    that, having regard to the purpose for which the information is to be used, the health
    information it collects, uses, holds or discloses is accurate, complete, up to date and
    relevant to its functions or activities.

4. Principle 4 - Data Security and Data Retention

4.1 An organisation must take reasonable steps to protect the health information it holds
    from misuse and loss and from unauthorised access, modification or disclosure.

4.2 A health service provider must not delete health information relating to an individual,
    even if it is later found or claimed to be inaccurate, unless:

   (a) the deletion is permitted, authorised or required by the regulations or any other
       law; or

   (b) the deletion is not contrary to the regulations or any other law and occurs:

       (i) in the case of health information collected while the individual was a
           child, after the individual attains the age of 25 years; or

       (ii) in any case, more than 7 years after the last occasion on which a health
           service was provided to the individual by the provide

           whichever is the later.

4.3 A health service provider who deletes health information in accordance with HPP 4.2
    must make a written note of the name of the individual to whom the health information
    related, the period covered by it and the date on which it was deleted.

4.4 A health service provider who transfers health information to another individual or
    organisation and does not continue to hold a record of that information must make a
    written note of the name and address of the individual or organisation to whom it was
    transferred.
4.5 An organisation other than a health service provider must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any other purpose authorised by this Act, the regulations made under this Act or any other law.

5. **Principle 5 - Openness**

5.1 An organisation must set out in a document:

(a) clearly expressed policies on its management of health information; and

(b) the steps that an individual must take in order to obtain access to their health information. The organisation must make the document available to anyone who asks for it.

5.2 On request by an individual, an organisation must take reasonable steps:

(a) to let the individual know:

   (i) whether the organisation holds health information relating to the individual; and

   (ii) the steps that the individual should take if the individual wishes to obtain access to the information; and

(b) if the organisation holds health information relating to the individual, to let the individual know in general terms:

   (i) the nature of the information; and

   (ii) the purposes for which the information is used; and

   (iii) how the organisation collects, holds, uses and discloses the information.

6. **Principle 6 - Access and Correction**

**Access**

6.1 If an organisation holds health information about an individual, it must provide the individual with access to the information on request by the individual in accordance with Part 5, unless:

(a) providing access would pose a serious threat to the life or health of any person under section 26 and refusing access is in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(b) providing access would have an unreasonable impact on the privacy of other individuals and refusing access is in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or
(c) the information relates to existing legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery in those proceedings or is subject to legal professional privilege; or

(d) providing access would reveal the intentions of the organisation in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the organisation unreasonably to disadvantage; or

(e) the information is subject to confidentiality under section 27; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

(h) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(i) providing access would be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency; or

(j) a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia; or

(k) the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again; or

(l) the individual has been provided with access to the health information in accordance with Part 5 and is making an unreasonable, repeated request for access to the same information in the same way.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than access to the information.

Note: An organisation breaches HPP 6.1 if it relies on HPP 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where HPP 6.2 does not apply.

6.3 If access is refused on the ground that it would pose a serious threat to the life or health of the individual, the procedure in Division 3 of Part 5 applies.

6.4 Without limiting sections 26 and 27, nothing in this Principle compels an organisation to refuse to provide an individual with access to his or her health information.

Correction

6.5 If an organisation holds health information about an individual and the individual is able to establish that the information is inaccurate, incomplete, misleading or not up to date,
6.6 If:

(a) the organisation is not willing to correct the health information in accordance with a request by the individual; and

(b) no decision or recommendation to the effect that the information should be corrected wholly or partly in accordance with the request, is pending or has been made under this Act or any other law; and

(c) the individual gives to the organisation a written statement concerning the requested correction

the organisation must take reasonable steps to associate the statement with the information.

6.7 If the organisation accepts the need to correct the health information but:

(a) the organisation considers it likely that leaving incorrect information, even if corrected, could cause harm to the individual or result in inappropriate health services or care being provided; or

(b) the form in which the health information is held makes correction impossible; or

(c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so corrected

the organisation must place the incorrect information on a record which is not generally available to anyone involved in providing health services to the individual, and to which access is restricted, and take reasonable steps to ensure that only the corrected information is generally available to anyone who may provide health services to the individual.

6.8 If an organisation corrects health information about an individual, it must:

(a) if practicable, record with the correction the name of the person who made the correction and the date on which the correction is made; and

(b) take reasonable steps to notify any health service providers to whom the organisation disclosed the health information before its correction and who may reasonably be expected to rely on that information in the future.

6.9 If an individual requests an organisation to correct health information about the individual, the organisation must take reasonable steps to notify the individual of a decision on the request as soon as practicable but in any case not later than 30 days after the request is received by the organisation.
**Written reasons**

6.10 An organisation must provide written reasons for refusal of access or a refusal to correct health information.

7. **Principle 7 - Identifiers**

7.1 An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

7.2 Subject to HPP 7.4, a private sector organisation may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector organisation (or by an agent of, or contractor to, a public sector organisation acting in its capacity as agent or contractor) if:

   (a) the individual has consented to the adoption of the same identifier; or
   
   (b) the use or disclosure of the identifier is required or authorised by or under law.

7.3 Subject to HPP 7.4, a private sector organisation may only use or disclose an identifier assigned to an individual by a public sector organisation (or by an agent of, or contractor to, a public sector organisation acting in its capacity as agent or contractor) if:

   (a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more of paragraphs (c) to (l) of HPP 2.2; or
   
   (b) the individual has consented to the use or disclosure; or
   
   (c) the disclosure is to the public sector organisation which assigned the identifier to enable the public sector organisation to identify the individual for its own purposes.

7.4 If the use or disclosure of an identifier assigned to an individual by a public sector organisation is necessary for a private sector organisation to fulfil its obligations to, or requirements of, the public sector organisation, a private sector organisation may either:

   (a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector organisation; or
   
   (b) use or disclose an identifier of the individual that has been assigned by the public sector organisation.

8. **Principle 8 - Anonymity**

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9.1 An organisation may transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles; or

(g) the transfer is authorised or required by any other law.

10. Principle 10 - Transfer or closure of the practice of a health service provider

10.1 This Principle applies if the practice or business of a health service provider ('the provider') is to be:

(a) sold or otherwise transferred and the provider will not be providing health services in the new practice or business; or

(b) closed down.

10.2 The provider or, if the provider is deceased, the legal representatives of the provider, must:

(a) publish a notice in a newspaper circulating in the locality of the practice or business stating:
(i) that the practice or business has been, or is about to be, sold, transferred or closed down, as the case may be; and

(ii) the manner in which the provider proposes to deal with the health information held by the practice or business about individuals who have received health services from the provider, including whether the provider proposes to retain the information or make it available for transfer to those individuals or their health service providers; and

(b) take any other steps to notify individuals who have received a health service from the provider in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph.

10.3 Not earlier than 21 days after giving notice in accordance with HPP 10.2, the person giving the notice must, in relation to health information about an individual held by, or on behalf of, the practice or business, elect to retain that information or transfer it to:

(a) the health service provider, if any, who takes over the practice or business; or

(b) the individual or a health service provider nominated by him or her.

10.4 A person who elects to retain health information must continue to hold it or transfer it to a competent organisation for safe storage in Victoria, until the time, if any, when the health information is destroyed in accordance with HPP 4.

10.5 Subject to HPP 10.2, a person must comply with the requirements of this Principle as soon as practicable.

10.6 Despite any other provision of the Health Privacy Principles, a person who transfers health information in accordance with this Principle does not, by so doing, contravene the Health Privacy Principles.

10.7 If:

(a) an individual, in response to a notice published under HPP 10.2, requests that health information be transferred to him or her or to a health service provider nominated by him or her;

(b) the person who published the notice elects to retain the health information

the request must be taken to be;

(c) in the case of a request that the health information be transferred to him or her, a request for access to that health information in accordance with Part 5 or HPP 6; and

(d) in the case of a request that the health information be transferred to a health service provider nominated by him or her, a request for the transfer of that health information in accordance with HPP 11

and it must be dealt with in accordance with this Act.
10.8 This Principle operates subject to any other law, including the Public Records Act 1973.

10.9 For the purposes of HPP 10.1(a), a business or practice of a provider is transferred if:

(a) it is amalgamated with another organisation; and

(b) the successor organisation which is the result of the amalgamation is a private sector organisation.

11. **Principle 11 -Making information available to another health service provider**

11.1 If an individual:

(a) requests a health service provider to make health information relating to the individual held by the provider available to another health service provider; or

(b) authorises another health service provider to request a health service provider to make health information relating to the individual held by that provider available to the requesting health service provider

a health service provider to whom the request is made and who holds health information about the individual must, on payment of a fee not exceeding the prescribed maximum fee and subject to the regulations, provide a copy or written summary of that health information to that other health service provider.

11.2 A health service provider must comply with the requirements of this Principle as soon as practicable.

11.3 Nothing in Part 5 or HPP 6 limits the operation of this Principle.

11.4 For the purposes of HPP 10.7, this Principle applies to a legal representative of a deceased health service provider in the same way that it applies to a health service provider.
24. ANNEXURE F - HEALTH PRIVACY PRINCIPLES - AUSTRALIAN CAPITAL TERRITORY


The full text of the ACT HPPs are attached.
ANNEXURE F:

Principle 1 - Manner and purpose of collection of personal health information

1. A collector shall not collect personal health information for inclusion in a health record or in a generally available publication unless:

   (a) the information is collected for a lawful purpose that is directly related to a function or activity of the collector; and

   (b) the collection of the information is necessary for or directly related to that purpose.

2. A collector shall not collect personal health information by unlawful or unfair means.

3. Where personal health information or health records are required to be collected by someone as part of his or her employment for the management, funding or quality of a health service received by the consumer, then that person is allowed access to the information only for those purposes, unless these principles otherwise provide.

Principle 2 - Purpose of collection of personal health information to be made known

1. Subject to clause 2 of this principle, where:

   (a) a collector collects personal health information for inclusion in a health record or in a generally available publication;

   (b) the information is solicited by the collector from the consumer concerned;

   the collector shall take such steps (if any) as are reasonable in the circumstances to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the consumer is generally aware of;

   (c) the purpose for which the information is being collected;

   (d) if the collection of the information is required or authorised by law - the fact that the collection of the information is so required or authorised;

   (e) unless it is obvious from the circumstances of any health service provided - the identity of all members of the treating team who will have access to the consumer's personal health information;

   (f) the identity of any person to whom, or agency to which, the collector would, in accordance with the collector's usual practice, disclose the information for inclusion in a health record or in a generally available publication; and

   (g) if it is, to the knowledge of the collector, the usual practice of any such person or agency to pass on such information to other persons or agencies - the identity of each of those other persons or agencies.

2. The collector is not required to notify the consumer of the identity of individuals, or classes of individuals, who are employed by the collector and who are required for the...
management, funding or quality of the health service received by the consumer to handle health records or personal health information as part of their employment.

**Principle 3 - Solicitation of personal health information generally**

Where:

(a) a collector collects personal health information about a consumer for inclusion in a record or in a generally available publication;

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is collected;

(c) the information is relevant, up to date and accurate; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the consumer.

**Principle 4 - Storage and security of personal health information**

A record keeper who has possession or control of a health record shall ensure that:

(a) the record is protected, by such security safeguards as are reasonable in the circumstances, against:

(i) loss; and

(ii) unauthorised access, use, modification or disclosure; and

(iii) other misuse; and

(b) if the record is given to another person - everything reasonably within the power of the record keeper is done to prevent unauthorised use or disclosure of any information contained in the record.

**Principle 5 - Information relating to records kept by record keeper**

1. A record keeper who has possession or control of health records shall, subject to clause 2 of this principle, take such steps as are reasonable in the circumstances to enable any consumer to ascertain:

(a) whether the record keeper has possession or control of any health records, or personal health information, relating to the consumer; and

(b) if so:

(i) the nature of the records or information; and 126

(ii) the main purposes for which the records are, or the information is, used; and
(iii) the steps that the person should take if the person wishes to obtain access to the records or the information.

2. A record keeper is not required to give a person information if, under a law of the Territory (including this Act) or a law of the Commonwealth, the record keeper is required or authorised to refuse to give that information to the person.

**Principle 6 - Access to health records by persons other than the consumer**

1. A health service provider who is a member of a treating team may have access to the personal health information of a consumer so far as is reasonably necessary for the provision by that provider of a health service to that consumer.

2. If a person reasonably requires access, for the purpose of the management, funding or quality of a health service received, or being received, by a consumer, to personal health information relating to the consumer, the person may have such access, without the consent of the consumer, to the extent reasonably necessary for that purpose.

3. Except where required or authorised by:

   (a) a law of the Territory; or

   (b) a law of the Commonwealth; or

   (c) an order of a court of competent jurisdiction;

   a person or agency shall not require a consumer, whether directly or indirectly, to obtain or grant access to any health record relating to the consumer.

**Principle 7 - Alteration of health records**

1. A person shall not delete information from a health record, even where it is later found or claimed to be inaccurate, unless the deletion is part of a program of archival destruction.

2. A record keeper who has possession or control of a health record shall take such steps, by way of making appropriate corrections and additions as are reasonable in the circumstances, to ensure that the record is:

   (a) up to date and accurate; and

   (b) relevant to the purpose for which the information was collected or is to be used and to any other purpose that is directly related to that purpose.

3. Where:

   (a) the record keeper of a health record is not willing to amend that record, by making a correction or an addition, in accordance with a request by the consumer concerned; and
(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request is pending, or has been made, under a law of the Territory (including this Act) or a law of the Commonwealth,

the record keeper shall, if the consumer gives to the record keeper a written statement concerning the requested correction or addition, take such steps as are reasonable in the circumstances to include the statement in the record.

4. Where the record keeper accepts the need to amend the health record but:

(a) the record keeper considers it likely that leaving incorrect information on a health record, even if corrected, could cause harm to the consumer or result in incorrect health care treatment or assistance being provided; or

(b) the form in which the record is held makes correction impossible; or

(c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so amended,

the record keeper shall place the incorrect information on a record which is not generally available to the consumer's treating practitioner or treating team, and to which access is restricted, and take such steps as are reasonable in the circumstances to ensure that only the corrected copy is generally available to the practitioner or treating team.

**Principle 8 - Record keeper to check accuracy etc of personal health information before use etc**

1. A record keeper who has possession or control of a health record shall not use personal health information in that record without taking such steps (if any) as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is up to date and accurate.

2. Where a person gives information in confidence to a health service provider about a consumer, the provider shall:

(a) encourage the person to waive the requirement of confidentiality; and

(b) if the information remains confidential:

(i) record the information only if it is likely to assist in the treatment or care of the consumer; and

(ii) take such steps (if any) as are reasonable in the circumstances to ensure that the information is accurate and not misleading.

**Principle 9 - Limits on use of personal health information**

1. Except where personal health information is being shared between members of a treating team to the extent necessary to improve or maintain the consumer's health or to manage a disability of the consumer, a record keeper who has possession or control of a health
record that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the consumer has consented to use of the information for that other purpose; or

(b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a significant risk to the life or physical, mental or emotional health of the consumer or another person; or

(c) use of the information for that other purpose is required or authorised by:

(i) a law of the Territory; or

(ii) a law of the Commonwealth; or

(iii) an order of a court of competent jurisdiction;

(d) the purpose for which the information is used is directly related to the purpose for which the information was obtained; or

(e) the use of the information is related to the management, funding or quality of the health service received by the consumer.

2. In relation to the sharing of information among a treating team, unless it is obvious from the circumstances or context of the health service, the person in charge of the treating team shall inform the consumer of the identity of all members of the treating team who will have access to the consumer's personal health information.

3. The treating team leader is not required to notify the consumer of the identity of individuals, or of classes of individuals, who are required for the management, funding or quality of the health service received by the consumer to handle health records or personal health information.

**Principle 10 - Limits on disclosure of personal health information**

1. Except where personal health information is being shared between members of a treating team only to the extent necessary to improve or maintain the consumer's health or manage a disability of the consumer, a record keeper who has possession or control of a health record shall not disclose the information to a person or agency (other than the consumer) unless:

(a) the consumer is reasonably likely to have been aware, or made aware under principle 2, that information of that kind is usually passed to that person or agency; or

(b) the consumer has consented to the disclosure; or

(c) the record keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent risk to the life or physical, mental or emotional health of the consumer or of another person; or

(d) the disclosure is required or authorised by:
(i) a law of the Territory (including this Act);

(ii) a law of the Commonwealth; or

(iii) an order of a court of competent jurisdiction; or

(e) the disclosure of the information is necessary for the management, funding or quality of the health service received by the consumer.

2. In relation to the sharing of information among the treating team, unless it is obvious from the circumstances and context of the health service, the person in charge of the treating team shall inform the consumer about the identity of all members of the treating team who will have access to the consumer's personal health information.

3. The treating team leader is not required to notify the consumer of the identity of individuals or of classes of individuals, who are required for the management, funding or quality of the health service received by the consumer, to handle health records or personal health information.

4. A person, body or agency to whom information is disclosed under clause 1 of this principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

5. Where there is an emergency and a consumer is unable to give or withhold consent to the disclosure of personal health information, the treating health service provider may discuss relevant personal health information with an immediate family member of the consumer to the extent that it is reasonable and necessary to do so for the proper treatment of the consumer.

Principle 11 - Transfer or closure of practice of health service provider

1. This principle applies if the practice of a health service provider (the "provider") is, or is proposed to be:

(a) sold or otherwise transferred; or

(b) closed down.

2. The provider or, if the provider is deceased, the legal representatives of the provider, shall:

(a) publish a notice in a newspaper circulating in the locality of the practice stating that:

(i) the practice has been, or is about to be, transferred or closed down (as the case may be); and

(ii) the health records of the practice, other than those returned to a consumer or passed on to a nominated practitioner at the consumer's request, will be transferred to a specified person (being a person to whom clause 3 (a) or (b) of this principle applies) at a specified address; and
(b) take such other steps as are practicable to inform every such consumer:

(i) that the practice has been, or is about to be, transferred or closed down (as the case may be); and

(ii) about the arrangements (as stated in the notice under paragraph (a)) for dealing with those health records.

3. Not earlier than 21 days after giving notice in accordance with clause 2 of this principle, the person or persons giving the notice shall transfer each health record held by, or on behalf of, the practice:

(a) to the health service provider (if any) who takes over the practice;

(b) to a competent record keeper for safe storage in the Territory (until such time (if any) as the record is destroyed as part of a program of archival destruction); or

(c) to the consumer to whom the record relates or to a practitioner nominated by that consumer.

4. Subject to the restriction stated in clause 3 of this principle, a person shall comply with the requirements of this principle as soon as practicable.

5. Despite any other provision of these principles, a person who transfers a health record in accordance with this principle does not, by so doing, contravene these principles.

**Principle 12 - Transfer of consumer to another health service provider or of health service provider to another practice**

1. Where:

(a) a consumer transfers from one health service provider to another; or

(b) a health service provider transfers from one practice to another and a consumer continues to see the provider,

the record keeper shall, on request, provide the consumer's health record, or a copy or written summary of it:

(c) if paragraph (a) applies - to the health service provider to whom the consumer has transferred; or

(d) if paragraph (b) applies - to the relevant health service provider.

2. The amount of a fee that is chargeable for providing, in accordance with clause 1 of this principle, a copy of a health record, or a written summary of a health record, is:

(a) if the Minister determines, under section 34, a fee for the purposes of this principle - an amount not exceeding the amount of the fee so determined; or

(b) in any other case - nil.