

Educational excellence and Catholic Values

Policy Statement

Privacy Kit

Revised - August 2006

Based on the National Catholic Education Commission
and National Council of Independent Schools
Associations Privacy Manual as developed by Minter
Ellison Lawyers



Catholic Education Office
Diocese of Parramatta

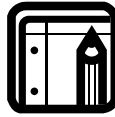
Acknowledgement

The National Catholic Education Commission and the National Council of Independent Schools worked closely with Minter Ellison Lawyers to assess the responsibilities of schools in relation to the introduction of the *Privacy Amendment (Private Sector) Act 2000* which amends the *Privacy Act 1988*.

A National Privacy Compliance Manual has been produced to assist non-government systems to implement the new Commonwealth privacy laws that came into effect on 21 December 2001. Schools may wish to access the manual which is available on the Catholic Education Commission website www.cecnsw.catholic.edu.au.

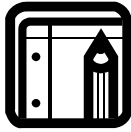
The Office of the Federal Privacy Commission provides valuable information on the new legislation through its website <http://www.privacy.gov.au>.

The Catholic Education Office has referred and applied the National Privacy Compliance Manual as developed by Minter Ellison Lawyers in preparing this kit for the use of schools, units and the Catholic Education Office in the Diocese of Parramatta.



CONTENTS

Section 1	The Privacy Act	page 3
Section 2	Complying with the Act	page 5
Section 3	Types of information	page 9
Section 4	The Privacy Policy	page 12
Section 5	Collection Notices	page 16
Section 6	Other requirements under the NPPs	page 23
Section 7	Some specific issues	page 31
Section 8	Privacy and students	page 33
Section 9	Privacy and contractors	page 35
Annexure A	<i>National Privacy Principles</i>	<i>page 37</i>
Annexure B	<i>School Counsellors and Privacy</i>	<i>page 44</i>



Section 1: The Privacy Act

The *Privacy Act 1988* is a Commonwealth Act that regulates the collection, storage, use and disclosure of different types of personal information by the Commonwealth and Australian Capital Territory government agencies, credit providers, credit reporting agencies and organisations that use tax file numbers.

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 came into effect on 21 December 2001.

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* governs how school and the Catholic Education Office must handle personal information.

Penalties

Schools and the Catholic Education Office will need to comply with the Act, or they may be liable to damages or required to comply with directions issued by the Privacy Commissioner. The Privacy Commissioner also has powers to publicise breaches of the *Privacy Act* in the media.

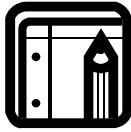
National privacy principles

A key component of the new legislation is the mandatory requirement for organisations to comply with ten (10) 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 following table summarises how the NPPs will apply to information which is held before, and information which is collected after, the commencement of the *Privacy Act* on 21 December 2001.

Privacy Kit

NPP	Topic	What information the NPP applies to:
NPP 1	Collection	only applies to information collected after 21 December 2001
NPP 2	Use and disclosure	only applies to information collected after 21 December 2001
NPP 3	Data quality and collection	only applies to information collected after 21 December 2001
NPP 3	Data quality on use and disclosure	applies regardless of when it was collected.
NPP 4	Data security	applies regardless of when information was collected
NPP 5	Privacy policies and openness	applies regardless of when information was collected
NPP 6	Access and correction	<p>if information already held is not used or disclosed it only applies to information collected after 21 December 2001, but, if information already held is used or disclosed after commencement then rights of access and correction apply unless</p> <ul style="list-style-type: none"> • unreasonable administrative burden or • cause the organisation unreasonable expense.
NPP 7	Commonwealth Government identifiers	applies regardless of when information is collected
NPP 8	Anonymity	only applies to information collected after 21 December 2001
NPP 9	Transborder data flow	applies regardless of when information is collected
NPP 10	Collection of sensitive information	only applies to information collected after 21 December 2001



Section 2: Complying with the Act

The following checklist will assist schools and the Catholic Education Office to comply with the requirements of the *Privacy Act*.

ITEM	REFERENCE/RESOURCE	CHECK ✓
Adoption of a Privacy Policy		
1. The system <i>Privacy Policy</i> has been reviewed to ensure that the school practices are in accord with the policy. 2. The system <i>Privacy Policy</i> has been displayed in a prominent place/s. Copies are available on request.	Privacy Kit–section 4, p12	
Appointment of a person/s responsible for privacy issues		
3. The principal has nominated a person on the Executive responsible for privacy (privacy contact person).	Privacy Kit – section 7, p30	
Revision of current information handling practices and amendment of all relevant documentation and forms		
4. A check has been made to ensure that personal and sensitive information collected from parents and students is 'necessary' for school activities.	Privacy Kit- section 3, p9 and section 6, p22	
5. A check has been made to ensure collection of information occurs in ways that are fair and not intrusive.	Privacy Kit – section 6, p22	
6. The following Collection Notices have been prepared for use on school letterhead Standard Collection Notice Alumni Collection Notice Employment Collection notice Contractor Collection Notice Volunteer Collection Notice.	Privacy Kit- section 5, p16	

Privacy Kit

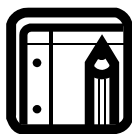
7. A copy of the <i>Standard Collection Notice</i> is provided annually to all parents.	Privacy Kit section 5, p 17	
8. The <i>Standard Collection Notice</i> is provided with all new enrolment forms.	Privacy Kit section 5, p17	
9. The <i>Standard Collection Notice</i> is publicised e.g. school diary, website, enrolment forms.	Privacy Kit section 5, p 16 & 17	
10. The <i>Alumni Collection Notice</i> is issued to past students (where relevant).	Privacy Kit section 5, p18	
11. An <i>Employment Collection Notice</i> is issued with employment application forms and in reply to unsolicited job applications, if they are retained. Employment practices are reviewed in the light of the Act.	Privacy Kit section 5, p19 and section 7, p30	
12. All contractors are given a copy of the <i>Contractors Collection Notice</i> and their contractual arrangements are reviewed	Privacy Kit section 5, p20 and section 9 p34	
13. All volunteers are given a copy of the <i>Volunteers Collection Notice</i> .	Privacy Kit section 5, p 21	
14. A script has been prepared based on <i>Standard Collection Notice</i> to comply with requirements for collection of information by telephone.	Privacy Kit section 5, p17	
15. Appropriate steps have been taken to comply with requirements related to disclosure of non-sensitive information for direct marketing (where relevant).	Privacy Kit section 6, p24	
Education of all staff and personnel		
16. The <i>Privacy Policy</i> is available to all employees.	Privacy Kit – section 4, p12	
17. Explanatory information sessions on the policy have been conducted for all existing staff and relevant personnel.	Training package on website	
Checking data quality		
18. The school has established standard procedures to ensure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.	Privacy Kit – section 6 & 7	

Privacy Kit

19. A disposal / retention system has been developed for all records containing information of a personal nature.	Privacy Kit – section 6 & 7	
20. Procedures are adopted to ensure that: (a) Records containing sensitive information such as health information are checked for accuracy before being used or relied upon. (b) A regular audit of all records of personal information is held whereby records that are not used are disposed of and inaccurate records updated. (c) Records no longer needed by the school are de-identified or destroyed. (d) An opportunity is made for the provider of information to update and ensure the accuracy of their personal information.	Privacy Kit – section 6 & 7	
Checking data security		
21. Hard copy records are secured in locked cabinets with restricted access. Building alarms or similar security measures are in place.	Privacy Kit – section 6, p24	
22. Steps have been taken to ensure that unauthorised access to personal information is minimised.	Privacy Kit – section 6	
23. Security of students/families personal information has been checked.	Privacy Kit – section 6	
24. Steps have been taken to ensure that personal information contained in databases is appropriately secure.	Privacy Kit – section 6	
25. Policies and security measures in respect of computer, email and internet use are in place.	Privacy Kit – section 6, p25 Use of internet and email	
26. Staff and other individuals with access to personal information have been informed as to the appropriate manner in which personal information should be treated.	Privacy Kit – section 6	
27. Reasonable steps have been taken to ensure that information provided over the internet is secure.	Privacy Kit – section 6, p24 Use of internet policy	

Privacy Kit

28. Reasonable steps have been taken to ensure that email communication and personal information contained therein is secure.	Privacy Kit – section 6, p24 Use of internet policy	
Providing access and correction		
29. The school has established a standard procedure for parents/students to have access to their personal information, except where denial is permitted.	Privacy Kit – section 6, p26 & 27 and section 8 p32 & 33	
30. A check has been made to ensure that identifiers such as a Medicare Number, a Social Security number or a Tax File Number are not used to identify an individual.	Privacy Kit – section 6, p 28	
31. Wherever practicable, parents and students have the option of remaining anonymous when providing information.	Privacy Kit – section 6, p 28	
Transferring information overseas		
32. The school has procedures in place for ensuring requirements are complied with when circumstances of transferring personal information overseas arise.	Privacy Kit – section 6, p28	
Complaints handling procedure and breach of NPPs		
33. The school has in place, in conjunction with its <i>Privacy Policy</i> , procedure for handling complaints about breaches.		
Ongoing compliance		
34. Ongoing compliance is monitored annually through the school journal process and in more detail through the school review process.		



Section 3: Types of information

What is personal information?

The *Privacy Act* regulates personal information contained in a 'record'. Personal information is information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can be reasonably ascertained, from the information or opinion.

It can range from very detailed information such as medical records to other less obvious types of information such as an email address.

Personal information likely to be collected

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).

- (a) **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.
- (b) **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.
- (c) **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.
- (d) **For others:** Personal information might also be collected from other people such as committee members, volunteers or donors.

What is sensitive information?

Sensitive information is a type of personal information that is given extra protection. 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 (e.g. vegetarianism, atheism)
- membership of a professional or trade association (e.g. membership of a Law Society, or Certified Practising Accountants)
- membership of a trade union (eg Teachers' Federation)
- sexual preferences or practices
- criminal record

Sensitive information likely to be collected

The following kinds of sensitive information are likely to be collected and held by schools:

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.

For parents: religion, country of birth and nationality

For job applicants, staff members and contractors: trade union membership, place of birth, religion, religious education, criminal record check, Child Protection Act information, member of professional associations, country of birth and nationality.

More on 'sensitive information' can be found on page 30 of this kit.

What is health information?

Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual and the individual's expressed wishes about the provision of health services.

Health information likely to be collected

The following types of health information are likely to be collected and held by schools:

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).

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

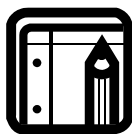
For job applicants, staff members and contractors: medical condition affecting ability to perform work, health information, compensation claims and doctor's certificates.

What is a 'record'?

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.

'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*.

There are some items which are excluded from the definition of 'record'. The exclusions relevant to the school are generally available publications (eg a telephone directory), and anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition



Section 4: The Privacy Policy

National Privacy Principle 5

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.

The Privacy Policy for schools and the Catholic Education Office in the Parramatta Catholic Education System is available for employees, pupils, parents and the broader community as required. The policy, below, was revised in August 2006.

Introduction

The Parramatta Catholic Education System is bound by the National Privacy Principles contained in the *Commonwealth Privacy Act* and is committed to upholding an individual's right to privacy and confidentiality particularly in regard to the collection and use of personal and sensitive information.

The *Privacy Policy* applies to all schools, the Catholic Education Office and other units which form part of the Parramatta Catholic education system.

The policy statement outlines how schools, the Catholic Education Office and other units use and manage personal information provided to or collected by them.

Associated documents

The policy statement entitled *Employee Use of Internet Facilities* provides advice to employees on the appropriate use of email and internet facilities.

The document/s entitled *Acceptable use of information technologies* provides advice to students on the appropriate use of email and internet facilities.

The document entitled *Protocols for Viewing Files* provides advice to employees wishing to view an investigation file relating to a matter pertaining to the *Ombudsman Amendment (Child Protection and Community Services) Act 1998*.

What kind of personal information is collected and how is it collected?

The type of information schools and the Catholic Education Office collect and hold includes, but is not limited to, personal information, including sensitive information, about:

- ◆ pupils and parents and/or guardians 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 and CEO.

Personal information provided by parents and students: 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* the National Privacy Principles do not apply to an employee record held by the employer. As a result, this privacy policy does not apply to the treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the employer and employee.

How is personal information used?

A school or the Catholic Education Office will use personal information it collects 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 parents or students have consented.

Pupils and Parents: In relation to personal information of pupils and parents, the primary purpose of collection is to enable the school to provide schooling for the pupil.

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

- ◆ keeping parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- ◆ engaging in day-to-day administration;
- ◆ looking after pupils' educational, social, spiritual and medical wellbeing;
- ◆ seeking donations and marketing for the school;
- ◆ satisfying the legal obligations of the Catholic Education Office and the schools;
- ◆ allowing 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, the primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor.

The purposes for which personal information of job applicants, staff members and contractors is used include:

- ◆ administering an individual's employment or contract;
- ◆ completing documentation for insurance purposes;
- ◆ seeking funds and marketing for the school;
- ◆ satisfying the legal obligations of the Catholic Education Office and the schools, in relation to child protection legislation for example.

Volunteers: A school obtains personal information about volunteers who assist the school in its functions or to conduct associated activities, such as alumni associations.

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, an 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 Parramatta Catholic education system schools and the Catholic Education Office to share personal (but not sensitive) information without issuing a standard collection notice, as they are part of the same legal entity. However, this personal information may only be used for the purpose for which it was originally collected. For example, when a pupil transfers from one school to another school in the Parramatta Catholic education system, personal information may be transferred.

Disclosing personal information

A school or the Catholic Education Office having issued a standard collection notice may disclose personal information, including sensitive information, held about an individual to:

- ◆ another school;
- ◆ government departments involved with schooling;
- ◆ the local parish;
- ◆ medical practitioners;
- ◆ people providing services to the school, including specialist visiting teachers and sports coaches;
- ◆ recipients of school publications prepared for the educational purposes of the school, like newsletters and magazines;
- ◆ parents;
- ◆ anyone parents or students authorise the school to disclose information to.

Sending information overseas: Personal information about an individual will not be sent 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.

Sensitive information

Sensitive information refers to information relating to: a person's racial or ethnic origin; political opinions; religion; trade union or other professional or trade association membership; sexual preferences; criminal record; and health information.

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

Management and security of personal information

All employees of the Parramatta Catholic education system are required to respect the confidentiality of pupils' and parents' personal information and the privacy of individuals.

Schools and the Catholic Education Office have in place steps to protect the personal information 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

Schools and the Catholic Education Office endeavour to ensure that the personal information is accurate, complete and up-to-date. A person may seek to update their personal information held by a school by contacting the school.

The National Privacy Principles require a school not to store personal information longer than necessary.

Consent and rights of access to the personal information of pupils

The Parramatta Catholic education 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 Catholic Education Office about them or their child. 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.

Pupils will generally have access to their personal information through their parents, but older pupils may seek access themselves. 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.

Seeking access to the personal information held by a school or the CEO

Under the *Commonwealth Privacy Act*, an individual may seek access to personal information which the school or the Catholic Education Office holds about them. There are some exceptions to this set out in the Act.

If a parent or student wishes to make a request to access any information the school or the Catholic Education Office holds about them, they are advised to contact the school's principal in writing, specifying the information that is requested.

The school may seek to verify the identity of the person seeking access to information. The school may charge a fee for access and will advise the likely cost in advance.

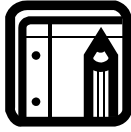
Enquiries

If you would like further information about the way your school or the Catholic Education Office manages the personal information it holds, please contact the school's principal.

Review

The Privacy Policy may be reviewed or updated from time to time to take account of new laws and technology, changes to schools' operations and practices and to make sure it remains appropriate to changing educational needs. A review of the policy will occur in 2009.

... End of policy...



Section 5: Collection notices

Requirements: 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:

- the organisation'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 that requires the collection of the information, and
- the main consequences, if any, of the individual not providing the information. (NPP1.3)

Organisations are required to ensure persons are advised of their rights pertaining to the collection of personal information. Schools can fulfil their obligations in relation to this requirement by issuing 'collection notices'.

Standard collection notice

The *Standard Collection Notice* will cover most situations requiring the collection of personal information by the school.

All parents should be sent a copy of the school's *Standard Collection Notice* at the beginning of each school year, perhaps when forwarding student information forms or school fee accounts.

It is advisable to publish the school's *Standard Collection Notice*, for example on the school website, student diary, enrolment forms.

Parents and students new to the school need to be given a copy of the *Standard Collection Notice* when completing enrolment forms.

It is sufficient for the school to distribute the collection notice. The school is not required to seek confirmation from parents that they have received the notice and accept the terms.

The following wording ensures the individual is reasonably aware of the matters specified in NPP 1.3 and also obtains 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.

STANDARD COLLECTION NOTICE

1. [NAME OF SCHOOL] in the Diocese of Parramatta collects personal information, including sensitive information, about pupils and parents or guardians before and during the course of a pupil's enrolment at [NAME OF 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 our 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. 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, the Catholic Education Office, the Catholic Education Commission, your local diocese and the parish, medical practitioners, and people providing services to the school, including specialist visiting teachers and counsellors, coaches and volunteers.
6. 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.
7. Personal information relating to pupils may be supplied to parishes for use by them for pastoral and fundraising purposes. If you object to the information being used in this manner, please contact the school.
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 and diocesan newsletters, magazines and websites.
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 or diocese's duty of care to the pupil, or where pupils have provided information in confidence.
10. As you may know from time to time the school 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 school and diocesan fundraising activities. We will not disclose your personal information to third parties for their own marketing purposes without your consent.
11. We may include your contact details in a class list and school directory.
12. If you provide us 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 we do not usually disclose the information to third parties.

Special note: Photos of children are used for various communication mediums including school and Catholic Education Office websites, school and system publications and newspapers, and enrolment posters. If any parent or guardian does not want their child's photo used in any of the above situations please inform the principal of the school in writing.

Verbal collection

If the school is collecting personal information by telephone, appropriate steps should be taken to make the individual aware of the matters contained in the *Standard Collection Notice* unless the person is already aware of these matters. In most cases the school would have already provided the individual with a copy of the *Standard Collection Notice* at the commencement of the school year and hence no further reference is required.

Alumni collection notice

At some schools, students' personal information is sent to the school's alumni or similar association when the pupil leaves the school. When this occurs the school should obtain the student's (or, if appropriate, the parent's) consent to this and should insert an appropriate collection notice in a relevant form (eg *Application for Membership of Alumni Association* form).

The Alumni Collection Notice is worded as follows:

ALUMNI COLLECTION NOTICE

1. [NAME OF ALUMNI ASSOCIATION] 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 [NAME OF 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 fundraising activities. If you do not agree to this, please advise us now.
4. [NAME OF ALUMNI ASSOCIATION] may publish details about you in our [NAME OF PUBLICATION]. If you do not agree to this, please advise us now.
5. You may seek access to personal information collected about you by contacting the association at [CONTACT DETAILS].
6. If you provide personal information to us about other people, we encourage you to inform them of the above matters.

Employment collection notice

When receiving employment applications an *Employment Collection Notice* should be sent to the individual.

If unsolicited job applications are received which the school wishes to retain, an *Employment Collection Notice* should be sent.

This *Employment Collection Notice* is worded as follows:

EMPLOYMENT COLLECTION NOTICE

1. In applying for this position you will be providing [NAME OF SCHOOL] of the Diocese of Parramatta 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 organization [IDENTIFY]. [PLEASE SELECT]
5. As required under NSW Child protection legislation, preferred applications for [INSERT POSITION TITLE] are required to be the subject of employment screening. This involves a check of relevant criminal history, any Apprehended Violence Orders, referee reports and employment history including disciplinary proceedings. Child protection legislation also requires that we collect a *Prohibited Employment Declaration* from you.
6. If you provide [NAME OF SCHOOL] with the personal information of others, we encourage you to inform them you are disclosing that information to us and why, that they can access that information if they wish, that we do not usually disclose the information to third parties.

Contractor and volunteer collection notice

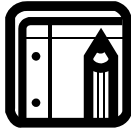
All new contractors and volunteers should be sent a modified version of the *Employment Collection Notice*. These notices are worded as follows:

CONTRACTOR COLLECTION NOTICE

1. In applying to provide your services you will be providing [NAME OF SCHOOL] of the Diocese of Parramatta with personal information. We can be contacted at [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. However, there may be occasions when access is denied.
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 under child protection legislation to collect information to ensure safety to students. The requirements will be dependent on the nature of your work. Specific details of our requirements will be provided prior to the commencement of work.
6. If you provide us with the personal information of others, we encourage you to inform them you are disclosing that information to us and why, that they can access that information if they wish, that we do not usually disclose the information to third parties.

VOLUNTEER COLLECTION NOTICE

1. In applying to provide your services you will be providing [NAME OF SCHOOL] of the Diocese of Parramatta with personal information. We can be contacted at [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. However, there may be occasions when access is denied.
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 under child protection legislation to collect information to ensure safety to students. The requirements will be dependent on the nature of your work. Specific details of our requirements will be provided to you prior to the commencement of work.
6. If you provide us with the personal information of others, we encourage you to inform them you are disclosing that information to us and why, that they can access that information if they wish, that we do not usually disclose the information to third parties.



Section 6: Other requirements under the National Privacy Principles

COLLECTION OF INFORMATION (NPP 1)

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

When is the collection of information 'necessary' for school activities?

It is recommended that all items of personal information that are collected by the school are identified and then reviewed as to whether their collection is necessary for one or more of the school's/CEO's functions.

For example, an 'Information Update' form completed by families may request the provision of the 'names and ages of all children in the family (including those who have left the school)'. It may be contended that the collection of information of this kind is not necessary for the functions and activities of the school. Alternatively, it might be possible to contend that this information is necessary because it is desirable for the school to have a complete profile of a pupil's family for educational and other reasons.

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

When might collection methods be considered 'unfair' or 'intrusive'? (NPP 1.2)

Examples of what might be considered unfair or unreasonably intrusive ways of collection include:

- covert collection (eg by surveillance camera)
- calling an individual late at night or at meal time without a prior arrangement to do so
- asking for information for one purpose when really it is for another purpose
- telling an individual that it is compulsory that they provide personal information when it is not, and
- asking for sensitive personal details within earshot of other people.

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

Where personal information is collected about an individual from someone else, the organisation must take reasonable steps to ensure the individual has consented.

Collect information directly (NPP 1.4 & 1.5)

In most cases schools will collect personal information directly from parents or students. The school may collect information indirectly from a third party such as the principal of another

school, doctors or government department. The *Standard Collection Notice* issued each year will cover most third party cases. If, however, the school considers that a certain situation goes beyond situations envisaged by the *Standard Collection Notice*, the school should contact the person to obtain their consent.

USE & DISCLOSURE OF INFORMATION (NPP 2)

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

- for the primary purpose for which it was collected, or
- for a secondary purpose related to the primary purpose of collection, or
- with the individual's consent, or
- for direct marketing where a number of requirements are met, or
- where the organisation reasonably believes that the use or disclosure is necessary to prevent threats to life, health or public safety; or
- where the organisation has reason to suspect that unlawful activity is being, or may be, engaged in, or
- where required or authorised by or under law; or
- the organisation reasonably believes the use or disclosure is necessary for the prevention, detection or investigation of crime or for legal proceedings.

When might use or disclosure of information not be reasonable?

Where a situation is not covered by a collection notice, use or disclosure of an individual's personal information might not be reasonably expected by the individual. Examples of such circumstances might be:

- displaying test/exam results (alongside names) on notice boards
- disclosing certain personal information about pupils or parents to other pupils or parents.

In some situations disclosure of information is required or authorised by law.

An example of where law requires the disclosure of personal information would be:

- where a *duty of care* requires a school to inform a third party in temporary charge of a pupil that the pupil suffers from a particular health problem and or disability
- where health laws require certain disclosures to public health authorities
- where child protection laws require certain disclosures to government authorities, and
- where the school is responding to unlawful activity e.g. communication with the police.

Using information for direct marketing

Direct marketing includes fundraising (eg direct requests, art unions, raffles), and sending advertising to individuals. The *Standard Collection Notice* addresses fundraising activities. If direct marketing communications are to be sent to people who have not been provided with the *Standard Collection Notice*, each direct marketing communication should include an 'opt-out clause' as follows:

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.

ENSURING THE QUALITY OF DATA (NPP 3)

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

Take proactive steps to have up-to-date information

One way of complying with NPP 3 is to maintain up-to-date and accurate records. This could be done by making available an annual 'update details' form or similar document to relevant individuals (eg enclosed with an invoice, school fees, newsletter or magazine, or contained on the school's website).

ENSURING DATA IS SECURE (NPP 4.1)

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

What level of security is required?

The level of security should be in proportion to the level of sensitivity of the personal information. For example, if a number of parents and pupils have access to an area which contains a list of childrens' names, their illnesses and medication requirements (such as on a notice board outside a classroom) then this would likely 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.

When leaving personal information unattended, reasonable steps should be taken to keep the information secure from unauthorised access. Examples include:

- locking unattended classrooms, cupboards and work areas
- using computer passwords (and changing them periodically)
- not leaving computers unattended where personal information may be accessible
- restricting access to staffrooms and offices to authorised personnel only

- ❑ securing information taken off school grounds (e.g. processing student records using remote online access or marking student work at home).

Use of internet and email

Schools need to have in place policies and security measures in respect of computer, email and internet usage (see system policies).

DESTROYING OR DE-IDENTIFYING DATA (NPP 4.2)

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.

When and how should records be destroyed or de-identified?

Destruction of records containing personal information needs to be by secure means. Ordinarily garbage disposal of intact documents is not secure, while shredding, pulping and confidential locked bins would be considered secure. The reasonableness of steps taken to destroy personal information contained in electronic records will depend on the medium on which data is stored and the available methods for erasing.

If a school wishes to retain data for research, it may be possible to de-identify the personal information.

In determining whether information is no longer required the school should consider whether there is a legal requirement to retain the information, whether it is likely that the information will be required at a later date, and whether destroying the information would likely have a prejudicial effect on the school.

If 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 hard-copy records

The following extract from Chapter 9 the *Principal's Handbook* advises on the length of time records need to be retained. If further advice is required on specific records contact the Area Administrator.

Retention periods for student records

The register of attendance (ie. the roll) should be retained for a period of **seven** years after the last entry was made before archiving.

An additional requirement exists where a student has been involved in an accident or incident which may lead to legal proceedings. In this case the roll must be kept until that student attains **24 years of age**. This is because the student, on reaching adulthood, has six years in which to commence proceedings.

If a computer database is used to store the register of enrolments and attendances:

- a back-up disk must be updated each week,
- a print-out must be made on a yearly basis and retained for a **seven**-year period.

Notes explaining student absences should be kept for at least **seven** years.

A register of admission should be kept **permanently**.

From 1 January 2005* it will be a requirement of registration that a record is kept of:

- (a) the date of enrolment and previous school or pre-enrolment situation of any student aged 6 years or more who enrolls at the school;
- (b) the date at which enrolment ceases and destination of any student under 15 years of age who leaves the school; or
- (c) for a student younger than 15 years who leaves without a destination being recorded, the date at which enrolment ceases and evidence that a DET officer with school liaison responsibilities has been notified of the student's name, age and last known address.

* *Registration Systems and member Non-government Schools (NSW) Manual, May 2004.*

Student performance records, including reports, should be kept for **five** years or until a student about whom legal proceedings may occur turns 24.

Retention periods for documents of a financial nature are detailed in item 8.6 of the *School Financial Management Manual*.

Records of the enrolment, course details (i.e. primary, junior secondary or senior secondary) attendance and residential address(es) of overseas students must be retained until 2 years after they cease to be enrolled as overseas students in any Catholic school in NSW. As the only practical way to meet this legal requirement is to provide these details to the Catholic Education Office, these details must be forwarded to the CEO as each overseas student commences. Address details must be updated while the overseas student is at the school concerned.

ACCESS TO DATA & CORRECTION OF DATA (NPP 6)

Requirement: An organisation must on request provide the individual with access to his or her own personal information and correct any inaccuracies. However, there are some exceptions to this requirement:

- **Where access is desired, the organisation must, where reasonable, consider whether the use of intermediaries would allow sufficient access.**
- **Reasons must be given where access is denied.**

When might it not be appropriate to provide access to personal information?

Examples of where access requests may be refused under NPP 6 include where:

- access would unreasonably impact on the privacy of other individuals e.g. a 'Report by Pupil Form' regarding an incident which included reference to other pupils who are the subject of the incident and report (e.g. in the case of bullying). In such cases partial access may be appropriate.)
- the request is frivolous or vexatious e.g. repeated request for the same information

- ❑ the information relates to existing or anticipated legal proceedings between the parties, and the information would not be accessible through discovery
- ❑ access would reveal a negotiation position e.g. in some cases regarding job applicants - although the 'employment collection notice' should cover this
- ❑ access would be unlawful e.g. it would breach a duty of confidence
- ❑ denying access is required or authorised by or under law e.g. confidential information may be withheld 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.
- ❑ access is likely to prejudice the investigation of a possible unlawful activity e.g. the investigation of an incident concerning a pupil, and
- ❑ access is likely to prejudice the prevention, detection, investigation, prosecution or punishment of an unlawful activity, by a law enforcement agency.

How can 'access' to information be provided?

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
- ❑ giving the person a print out of the information if it is in electronic form, and
- ❑ giving the individual a summary of the information.

What steps need to be taken when access to information is requested?

Usually records of personal information which the school or CEO creates will be the property of the school/CEO. The following are a number of matters that might be considered when an access request is made

- ❑ If the information was collected before 21 December 2001 (and not subsequently updated, used or disclosed), then NPP 6 will not apply and access may be denied
- ❑ Verify the identity of the individual and clarify the information sought.
- ❑ Consider what information the individual wants to access and whether the exceptions require the school/CEO to refuse access.
- ❑ Consider the most appropriate form of access eg allowing the individual to inspect the information, providing a photocopy, providing an accurate summary.
- ❑ A charge for access may be made, but it must not be excessive.

IDENTIFIERS (NPP 7)

Requirement: Identification devices provided by a government agency, such as a Medicare number, cannot be used by an organisation as its own identifier to

identify an individual.

Examples of agency issued identifiers which may not be used to identify an individual are Medicare number, Tax File Number, Social Security number, Passport number:

Examples of identifiers not regulated by the Act which may be used are ABN, driver's licence number, a person's name or initials, unique numbers created by the School (e.g. payroll number)

ANONYMITY (NPP 8)

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

When might this situation apply?

As most 'transactions' would require a person's details, it would appear that NPP 8 is of little significance to schools and the CEO. Examples of where individuals would be able to remain anonymous might be:

- ❑ 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
- ❑ where an individual requests a prospectus and it can be provided without collecting the individual's personal information (eg at an 'open day'), and
- ❑ where surveys are conducted where there is no need to collect a respondent's personal information such as their name and address.

TRANSBORDER DATA FLOWS (NPP 9)

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 when the individual consents to the transfer.

When might this situation apply?

Examples of transferring personal information overseas include:

- ❑ situations involving Full Fee Paying Overseas Students (FFPOS)
- ❑ the sending of information about a pupil to an overseas school for an exchange program
- ❑ the sending of school reports, invoices and other material to parents and other parties located overseas, and
- ❑ marketing the school to people overseas by sending them material containing personal information.

What should the school or CEO do in such cases?

Information transferred directly to the parent or student will be covered by the *Standard Collection Notice*.

If the transfer of information needs to be via a third party intermediary, it would be necessary to obtain consent from the parents or pupil for the transfer. This could simply be done by amending the *Standard Collection Notice* to include the following sentence:

We may transfer any or all of this information to a third party, whether in Australia or overseas, for the following purposes [INSERT PURPOSE e.g. provide information about the school]

SENSITIVE INFORMATION (NPP 10)

- **Requirement: In general an organisation should not collect sensitive information about an individual, unless an applicable exception applies. The exceptions include where:**
 - the individual has consented
 - collection is required by law
 - 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
 - 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
 - other specific circumstances exist for sensitive information which is health information.

What information would be required by law?

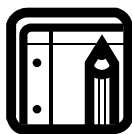
Examples of collection as required by law include:

- immunisation records and information requested in enrolment and various medical forms (eg as required under the public health legislation), and
- checks on criminal records, AVOs, and whether certain offences (eg certain sexual offences) have been committed in order to determine whether a job applicant is a 'prohibited person' under the *Child Protection (Prohibited Employment) Act 1988* (NSW).

Does the *Standard Collection Notice* cover sensitive information?

The *Standard Collection Notice* is designed to cover most circumstances. For example, 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, consent to the school's collection might be implied.

If, however, a school considers that some instances of collection goes beyond the situations envisaged in the *Standard Collection Notice*, then it should get an assurance from the third party that the individual has consent to the school's collection or should otherwise obtain the individual's consent directly.



Section 7:

Some specific issues for schools and the Catholic Education Office

EMPLOYEE RECORDS EXEMPTION

Employee records of current or former employees are exempt from the scope of the *Privacy Act*. An 'employee record' is broadly defined as a record held by the employer of personal information relating to the employment of an employee.

Hence employers are not required to issue employees with *Standard Collection Notices*. It is understood however, that schools and the Catholic Education Office engage in practices which ensure the personal information of employees is handled confidentially.

It might be argued that some practices in relation to employees could possibly fall outside the employee record exemption. For 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. Such situations would be considered on a case by case bases. The employee records exemption is lost when the record is passed on to a third party or organisation, such as an independent legal entity.

JOB APPLICANTS

The employee records exemption does not apply to job applicants. Therefore under NPP 6 job applicants may seek access to records of personal information held by the school or Catholic Education Office. The school / CEO needs to be mindful of this when collecting personal information, e.g. references, interview notes and reports. Documents which are not required should be destroyed when the position has been filled.

Where a job applicant includes the name of a referee on their application it can be implied that they consent to the school /CEO contacting the person to collect personal information about them. However, if the school/CEO wishes to collect information from a referee or third party not identified on the application, the school should obtain the applicants consent to collect the information from that person. If the applicant declines to give consent and this may prejudice their applicant they need to be informed of this. This may occur, for example, if the applicant has not identified their immediate employer as a referee as the CEO *Employment Eligibility Form* requires a reference check with the immediate employer.

ROLE OF PRIVACY CONTACT PERSON

Although not required under the Act, the school should consider clearly identifying in allocated roles, the person on the executive responsible for ensuring the school is complying with privacy legislation. The principal may be the person who assumes this role or may delegate the responsibility to another member of the executive.

The person appointed to the role should be familiar with the Privacy Policy and should ensure the school is compliant with the requirements of the legislation. The person would initially review current information handling practices used by the school.

PASSING INFORMATION IN A SCHOOL COMMUNITY

The school community will typically consist of staff, pupils, parents, past pupils, benefactors, priest/s and parish community/ies.

As in any community, information about others is passed on through the community and on occasions will be recorded. For example, a note from the 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 the passing on the information would be expected, there it is unlikely to be any repercussions.

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. 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.

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.

SCHOOL DIRECTORIES

School directories and class lists which contain students' and parents' name and contact numbers, 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. The *Standard Collection Notice* includes a clause asking parents to advise the school if they do not wish their contact details to be published.

SCHOOL PUBLICATIONS

Ideally, personal information which is collected for inclusion in a school publication should be collected directly from the individual concerned, particularly where the information relates to personal or private matter.

Where this is impracticable, the *Standard Collection Notice* does provide advice on collection practices. A copy of the publication should be provided to the individual.

PUBLISHING YEARBOOKS ON DISC

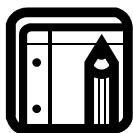
Yearbooks may be published as a disc but should be produced as 'read only'. A statement should accompany the disc outlining that it is not to be copied. Copying may infringe both privacy and copyright laws.

LIBRARY COLLECTIONS

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

PARRAMATTA CATHOLIC EDUCATION SYSTEM

The system involves the conduct of a number of schools by the one diocesan legal entity. Each Diocese is incorporated by an Act of Parliament and is created as a separate legal entity. Personal information can be used across schools and the Catholic Education Office within the Parramatta Catholic education system for the purpose for which it is collected as it is a single legal entity.



Section 8: Privacy and students

What does the *Privacy Act* require?

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.

The Privacy Commissioner states on 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.

What is the school's obligation to parents?

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.

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.

A 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.

For these reasons, it is suggested that in most 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.

When would consent be sought directly from students?

A school needs to recognise that young people do have rights under the *Privacy Act* and in some circumstances it would be appropriate to seek consent from them, particularly when they are older. 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.

It would usually be appropriate for the school to collect personal (and sensitive) information directly from a mature student. 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 (e.g. during day to day classroom activities).

Do students need to receive *standard collection notices*?

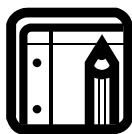
If parents are given a collection notice informing them of the requirements set out in NPP 1.3, pupils do not have to be specifically informed. A good practice, however, would be to include the notice in the student diary.

Duty of care and obligations of confidentiality

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. 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.

The common law, in some situations, imposes upon people an obligation of confidence. However, the NPPs appear to require personal information to be disclosed except where a specific exemption applies. 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. 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.



Section 9: Privacy and contractors

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

Contractors

Schools and the Catholic Education Office sometimes enter into contractual relationships with another party (the contractor) in which the contractor supplies services to the school, or supplies services to someone else on behalf of the school, and the contract involves the contractor handling personal information.

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.

Contracting with businesses not covered by the Privacy Act

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.

Disclosure to contractors

Where the school and a contractor are separate entities under the *Privacy Act*, when the school gives personal information to a contractor it discloses 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.

When the school contracts out functions or activities, both the school and the contractor have obligations under the Act to take reasonable steps to make an individual aware of certain information. These are covered separately below.

The contracting organisation (school)

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. 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 *Standard Collection Notice* the following statement:

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.

The contractor

There are a number of ways in which a contractor collecting personal information under a contractual arrangement could meet its obligations. What are reasonable steps will depend on the circumstances. The contractor does not necessarily need to notify individuals as the school may have already advised them that information will be disclosed to the contractor, the purpose for which the contractor will use the information, and how individuals can contact the contractor.

It may be reasonable for the contractor to take no action. An example of this could be where all of the following apply:

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

Use and disclosure

Where the school contracts out a function or activity for the school's primary purpose or an activity that is related to the primary purpose and within the individual's reasonable expectations, the *Standard Collection Notice* will suffice.

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.

Reduce risks through clear contracts

One way for schools and the CEO to reduce this risk is to ensure that contracts include very clear provisions about the purpose for which the contractor is to use 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.



Annexure A - National privacy principles

Annexure C is the full text of the NPPs as contained in Schedule 3 to the Privacy Act. The NPPs and the Privacy Act is contained on the Privacy Commissioner's website:
<http://www.privacy.gov.au/>.

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;
- (vi) 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.

7.2 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).

7.3 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).

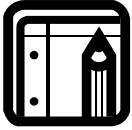
- 7.4 In this clause:
'identifier' includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not 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.



Annexure B – School counsellors and privacy

1. Introduction

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. It is important to note that:

- (a) Counsellors do not enjoy any general “legal professional privilege”
- (b) Counsellors must respond to Summons and Subpoenas
- (c) Counsellors have to maintain the confidence of their clients in the context of an ethical (not just a legal) relationship.

The Criminal Procedure Act 1986 (“the Act”) has been amended by the *Criminal Procedure Amendment (Sexual Assault Communications Privilege) Acts 1999 and 2002*. In broad terms, communications in confidence between counsellors and victims of sexual assault, referred to in the new act as “protected confidences”, are exempt from production under subpoena subject to certain exceptions.

The court can order the production of the material if satisfied of the following:

- (i) the documents have substantive probative value, i.e. they will provide significant assistance in establishing particular facts
- (ii) other evidence of the protected confidence 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.

2. 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.

3. Effect of employment status of counsellors

3.1 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.

3.2 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.

3.3 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.

4. 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.

5. 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.

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.

There may also be occasions where disclosure is prohibited because of the school's obligation under Child Protection Legislation.

... END OF PRIVACY KIT ...