

APPLICABLE TO	All employees of the CSO and diocesan schools
DOCUMENT OWNER	Director of Schools
APPROVAL DATE	November 2017
APPROVED BY	Director of Schools
SCHOOL ACTIONS	System Policy – Each school is to develop its own Privacy Management Procedure consistent with and aligned to the principles and practices outlined in this policy. Local policy not required.
LAST REVIEW DATE/S	September 2016
NEXT REVIEW DATE	March 2018
RELATED DOCUMENTS	Collection Notices: Standard, Employment Collection Notice, Enrolment Information Collection Notice, Volunteer/Contractor Collection Notice Complaints & Grievances Resolution Policy 2013 Confidentiality of Employees Policy 2016 Confidentiality Agreement – Employees Consent to Use Student Materials Disclosure Statement to Students – Counselling Services Photograph/Video Permission Form (Students, Employees) Privacy Breach Response Procedure 2016 Privacy Complaint: Internal Review Guidelines Privacy Management Procedure 2016 Workplace Internet, Email and Network Usage Policy May 2013

Purpose

This policy aims to ensure that the CSO and schools conducted by the CSO comply at all times with their obligations under the *Privacy Act 1988* (Cth) as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

Policy Statement

This policy sets out how personal information provided to or collected by the CSO and its schools is managed.

The CSO is bound by the Australian Privacy Principles (APPS) contained in the Commonwealth *Privacy Act 1988*. In relation to health records, the CSO is also bound by the Health Privacy Principles contained in the *Health Records and Information Privacy Act 2002*.

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

Scope

This policy covers the CSO and all diocesan schools.

Guiding Principles

3.1 COLLECTION OF PERSONAL INFORMATION

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

- students and parents and/or guardians (Parents) before, during and after the course of a student's enrolment at the school:
 - name, contact details (including next of kin), date of birth, previous school and religion
 - medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors)
 - conduct and complaint records, or other behaviour notes, and school reports
 - information about referrals to government welfare agencies
 - counselling reports
 - health fund details and Medicare number
 - any court orders
 - volunteering information
 - photos and videos at school events
- job applicants, staff members, volunteers and contractors, including:
 - name, contact details (including next of kin), date of birth, and religion
 - information on job application
 - professional development history
 - salary and payment information, including superannuation details
 - medical information (e.g. details of disability and/or allergies, and medical certificates)
 - complaint records and investigation reports
 - leave details
 - photos and videos at school events
 - workplace surveillance information
 - work emails and private emails (when using work email address) and Internet browsing history
- other people who come into contact with the school, including name and contact details and any other information necessary for the particular contact with the school.

Personal information provide by individuals: The CSO and a school will generally collect personal information held about an individual by way of forms filled out by parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than parents and students provide personal information.

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

Exception in relation to employee records: Under the *Privacy Act* and *Health Records and Information Privacy Act 2002* (NSW), the Australian Privacy Principles and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the CSO or school's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the CSO/school and employee.

3.2 HOW THE CSO/SCHOOL USES PERSONAL INFORMATION

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

Students and parents: In relation to personal information of students and parents, a school's primary purpose of collection is to enable the school to provide schooling for students enrolled at the school, exercise duty of care, and perform necessary associated administrative activities, which will enable students to take part in all the activities of the school. This includes satisfying the needs of parents, the needs of the student and the needs of the CSO and school throughout the whole period the student is enrolled at the school.

The purposes for which the CSO and a school use personal information of students and parents include:

- keeping parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines
- day-to-day administration
- looking after students' educational, social, spiritual and medical wellbeing
- seeking donations and marketing for the school
- satisfying the CSO and the school's legal obligations and allowing the school to discharge its duty of care

In some cases where a school requests personal information about a student or parent, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

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

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

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

Volunteers: Personal information about volunteers who assist the school in its functions or conduct associated activities, such as alumni associations, is obtained to enable the school and the volunteers to work together.

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

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

Exception in relation to related schools: The Privacy Act allows each school, being legally related to each of the other schools conducted by the CSO, to share personal (but not sensitive) information with other schools conducted by the CSO. Other CSO schools may then only use this personal information for the purpose for which it was originally collected by the CSO. This allows schools to transfer information between them; for example, when a student transfers from one CSO school to another.

3.3 DISCLOSURE OF PERSONAL INFORMATION

A school may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools
- government departments
- the Catholic Education Office, the Catholic Education Commission, the school's local diocese and the parish, other related church agencies/entities, and schools within other dioceses
- the school's local parish
- medical practitioners
- people providing educational, support and health services to the school, including specialist visiting teachers, sports coaches, volunteers, counsellors and providers of learning and assessment tools
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority
- people providing administrative and financial services to the school
- recipients of school publications, such as newsletters and magazines
- students' parents or guardians
- anyone you authorise the school to disclose information to
- anyone to whom we are required to disclose the information by law, including child protection laws

Sending information overseas: A school may disclose personal information about an individual to overseas recipients, for example, to facilitate a school exchange. However, a school will not send personal information about an individual outside Australia without:

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

3.4 STORAGE OF PERSONAL INFORMATION

The CSO and its schools may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

Examples of such cloud service providers include Microsoft and Google. Microsoft Office 365 (O365) and Google Apps for Education (GAFE) store and process limited personal information for this purpose. School personnel and the CSO and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering O365 and GAFE and ensuring proper use.

3.5 TREATMENT OF SENSITIVE INFORMATION

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

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

3.6 MANAGEMENT AND SECURITY OF PERSONAL INFORMATION

Staff are required to respect the confidentiality of employee, students and parent personal information and the privacy of individuals.

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

3.7 ACCESS AND CORRECTION OF PERSONAL INFORMATION

Under the Commonwealth *Privacy Act* and *Health Records Act*, an individual has the right to seek and obtain access to any personal information which the CSO or a school holds about them and to advise the CSO or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Students will generally be able to access and update their personal information through their parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or update any personal information the CSO or a school holds about you or your child, please contact the CSO or school in writing.

The CSO or school may require you to verify your identity and specify what information you require. The school may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the CSO/school will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

3.8 CONSENT AND RIGHTS OF ACCESS TO THE PERSONAL INFORMATION OF STUDENTS

The CSO 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 student to the student's parents. A school will treat consent given by parents as consent given on behalf of the student, and notice to parents will act as notice given to the student.

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

A school may, at its discretion, on the request of a student grant that student access to information held by the school about them, or allow a student 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 student and/or the student's personal circumstances warrant it.

3.9 NAPLAN

All schools in Australia are required to participate in the National Assessment Program – Literary and Numeracy (NAPLAN). NAPLAN will move online from 2018 (with some limited readiness testing occurring from 2017). Schools will be required to provide notifications to parents in relation to NAPLAN online.

The Standard Collection Notice – Students reflects the personal information flows associated with NAPLAN online (including the potential disclosure by schools of parents' and students' personal information as part of NAPLAN online).

Schools will be provided with a separate NAPLAN online specific notice that schools will need to provide to parents. This notice will need to be provided to parents each year before NAPLAN testing commences (usually as part of an information pack with general information about NAPLAN).

3.10 USE OF GOVERNMENT RELATED IDENTIFIERS

A government related identifier (GRI) is an identification device provided by a government agency, such as a Medicare number, tax file number or driver's licence number. GRIs cannot be

- adopted by a school as its own identifier to identify an individual unless required or authorised by law.
- used or disclosed unless it is reasonably necessary to verify identification of the individual or to fulfil its obligations to an agency or state or territory authority.

Schools should follow these guidelines regarding using GRIs:

DO use identifiers which are created by the school to identify individuals, not GRIs.

DON'T create databases that allow an individual's GRI to be entered in order to retrieve a record about the individual.

DON'T leverage off GRIs as a means of tracking students throughout their schooling life.

3.11 ENQUIRIES AND COMPLAINTS

If you would like further information about the way the CSO or a school manages the personal information it holds, or wish to complain that you believe that the CSO or a school has breached the Australian Privacy Principles, please contact the school's principal or the CSO. The CSO or the school will investigate any complaint and will notify you of a decision in relation to your complaint as soon as is practicable after it has been made.

The information provided based on the questions below will assist the Catholic Schools Office in assessing and processing a privacy complaint.

1. Name and address of the school or office you are complaining about.
2. Your details – name, address, email address.
3. Are you making the complaint on behalf of someone else (e.g. parent of a student)?
4. What is the specific conduct you are complaining about?
5. Which of the following describes your complaint:
 - Collection of my personal or health information
 - Security or storage of my personal or health information
 - Refusal to let me access or find out about my own personal or health information
 - Accuracy of my personal or health information
 - Use of my personal or health information
 - Disclosure of my personal or health information
 - Other
 - Unsure
6. When did the conduct occur? Please be as specific as possible.

7. When did you first become aware of this conduct? Please be as specific as possible.
8. What effect did the conduct have on you?
9. What effect might the conduct have on you in the future?
10. What would you like to see done about the conduct?

Responsibilities

Director of Schools

The Director of Schools is responsible for ensuring the enactment of this policy and that the implementation of the policy and associated procedures is adequately resourced.

Catholic Schools Office Leadership Team

All members of the Catholic Schools Office Leadership Team are to ensure that all members of their teams are aware of and familiar with the policy and that all activities of their respective departments are compliant with this policy and the associated procedures.

Principals

All Principals of diocesan schools are to ensure that all staff at the school are aware of and familiar with their system's privacy policy and that all school activities are compliant with this policy and associated procedures.

Other Employees with Supervisory Responsibilities

All other employees of the Catholic Schools Office holding a supervisory position are to ensure that they are aware of and familiar with this policy and that all activities under their supervision are compliant with the policy and associated procedures.

All Employees

In addition to any responsibilities outlined above, all Catholic Schools Office and diocesan school employees are expected to comply with privacy requirements.

Budget

Each year an appropriate school budget is to be allocated for complaints management reflecting this policy and the priorities of the school system strategic plan. Diocesan and local budgets should support the appropriate training and professional development of staff.

Legislative/Professional Guidelines

Australian Privacy Principles January 2014

National Catholic Education Commission & National Council of Independent Schools' Associations

Privacy Act 1988

CECNSW Privacy Compliance Manual August 2017

Privacy Amendment (Enhancing Privacy Protection) Act 2012