TRINITY CATHOLIC SCHOOL
Enhancing Privacy Protection
Policy

Related Policies

Confidentiality

Purpose

This policy acknowledges that the Catholic Education Office (CEO) and System Schools are bound by the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988 (Cth)* as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and states the commitment of the CEO to respect the privacy rights of families, (parent/students) employees, and all individuals in the workplace, and those interacting with the CEO and System Schools. Furthermore, the policy has been established to ensure that all Catholic Education Office workers comply at all times with its obligations under the *Privacy Act 1988 (Cth)* as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

Policy

The guiding legislation for the CEO is stated above. In relation to health records, the CEO is also bound by ACT or NSW State and Territory legislation, for instance: Health Privacy Principles contained in the *Health NSW or ACT Records and Information Privacy Act 2002 (Health Records Act).* The most relevant segment of the Privacy Act to the CEO is the Australian Privacy Principles, which are contained within the Act. The CEO's policy on collection, use and control of personal information is at all times consistent with its obligations under the Act.

The CEO and System schools:
1. Manage personal information in an open and transparent way.
2. Take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to a school's or the CEO's functions or activities that:
(a) will ensure compliance with the Australian Privacy Principles (APPs)
(b) will enable the school and the CEO to deal with inquiries or complaints about compliance with the APPs.
3. Have a clearly articulated up-to-date Privacy Policy about the management of personal information.
4. Only collect personal information that is reasonably necessary for the functions or activities of System
Schools or the CEO.
5. Obtain consent to collect sensitive information unless specified exemptions apply.
6. Use fair and lawful means to collect personal information including health information of students, parents and staff.
7. Collect personal information directly from an individual if it is reasonable and practicable to do so.
8. If a school or the CEO receives unsolicited personal information, determine whether it could have collected the information under APP 3 as if it had solicited the information. If so, APPs 5-13 will apply. If not, the information must be destroyed or de-identified.
9. At the time a school or the CEO collects personal information or as soon as practicable afterwards,
take such steps (if any) as are reasonable in the circumstances to make an individual aware of:
(a) why information is collected

(b) who else the school or the CEO might give the information to
(c) action and correction procedures.
10. Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in APP 6.2 applies. For example, for a related secondary purpose within the individual's reasonable expectations, consent for other use is granted or there are specified law enforcement or public health and public safety circumstances.
11. If the information is sensitive, the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the primary purpose of collection.
12. Personal information will not be used for direct marketing, unless one of the exceptions in APP 7 applies. For example, the School has obtained consent or where the individual has a reasonable expectation of their information being used or disclosed for that purpose and the school or the CEO has provided a simple means for the individual to unsubscribe from such communications.
13. Before the school or the CEO discloses personal information to an overseas recipient it must take such steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs, unless an exception applies.
14. Take such steps (if any) as are reasonable in the circumstances to ensure the personal information the school or the CEO collects, uses or discloses is accurate, complete and up-to-date. This may require the school or the CEO to correct the information and possibly advise organisations to whom it has disclosed the information of the correction.
15. Take such steps as are reasonable in the circumstances to protect the personal information a school or the CEO holds from misuse, interference and loss and from unauthorised access, modification or disclosure.
16. Take such steps as are reasonable in the circumstances to destroy or permanently de-identify personal information no longer needed for any purpose for which the school or the CEO may use or disclose the information.
17. If requested, the school and the CEO must give access to the personal information it holds about an individual unless particular circumstances apply that allow it to limit the extent to which it gives access.
Note: This is a summary only and NOT a full statement of obligations.

Definitions

Personal information means:
Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
a. whether the information or opinion is true or not
b. whether the information or opinion is recorded in a material form or not.

Sensitive information means:
a. information or an opinion about an individual's:
    i. racial or ethnic origin
    ii. political opinions
    iii. membership of a political association
    iv. religious beliefs or affiliations
    v. philosophical beliefs
    vi. membership of a professional or trade association
    vii. membership of a trade union
    viii. sexual orientation or practices
    ix. criminal record that is also personal information
b. health information about an individual (including information about a disability or an ILP)
c. genetic information about an individual that is not otherwise health information

d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification
e. biometric templates.

Health information means:
Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service.

Record means:
The Privacy Act regulates personal information contained in a 'record'. A 'record' includes a 'document', whether in paper form or held in an electronic or other device. The definition in the Amending Act is inclusive and therefore now covers a wide variety of material which might constitute a record. A 'document' is defined to include anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs.
Summary of Relevant Australian Privacy Principles (APPs)

APP 1 — Open and transparent management of personal information:
This principle ensures that the schools and the CEO manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 3 — Collection of solicited personal information:
This principle outlines when schools and the CEO can accumulate personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information
This principle outlines how schools and the CEO must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information
This principle outlines when and in what circumstances schools and the CEO collects personal information, and when they must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information
This principle outlines the circumstances in which schools and the CEO may use or disclose personal information that it holds.

APP 7 — Direct marketing
This principle stipulates that an organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information
This principle outlines the steps schools and the CEO must take to protect personal information before it is disclosed overseas.

APP 10 — Quality of personal information
This Principle requires schools and the CEO to take reasonable steps to ensure the personal information it collects is accurate, up to date and complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information
This principle requires schools and the CEO to take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification

or disclosure. An entity also has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information
This principle outlines the obligations of schools and the CEO when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information
This principle outlines the obligations of schools and the CEO in relation to correcting the personal information it holds about individuals.

Procedures

The CEO acknowledges the obligations it has as an institution to individuals. It also recognises that the staff of the CEO and its schools may require access to personal information consistent with its professional responsibilities to other staff and students. This requirement brings with it an obligation for staff to understand and acknowledge the nature and limits of their access to and use of personal information.

Collecting Personal Information:
The type of information schools and the CEO collect and hold includes (but is not limited to) personal information, including health and other sensitive information about:
- students and parents and/or guardians before, during and after the course of a student's enrolment at the school
- job applicants, staff members, volunteers and contractors
- other people who come into contact with the school.

Providing personal information:
Schools and the CEO will generally collect personal information about an individual by way of forms filled out by parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasion people other than parents and students may provide personal information.

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

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

Using personal information:
System schools and the CEO will use personal information it collects for the primary purpose of collection, and for secondary purposes that could reasonably be expected to relate to the primary purpose of collection, including the discharge of the school's duty of care to its students, or for which the school or the CEO have obtained consent or are required by law, such as child protection.

Students and Parents:
In relation to personal information of students and parents, the primary purpose of collection by schools and the CEO is to enable them to provide schooling for the students. This includes

addressing the needs of parents, the needs of the student and the needs of the CEO and System schools throughout the whole period the student is enrolled in the System.

The purposes for which the CEO or a System School uses personal information of students and parents includes

- to keep 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
- to satisfy the CEO's and school's legal obligations, and allow the school to discharge its duty of care.
- to communicate with Archdiocesan and Parish bodies regarding matters concerning the school's religious Education Program.

In some cases where a school or the CEO requests personal information about a student or parent, if the information requested is not obtained, the school or the CEO 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
- fulfilling insurance purposes
- satisfying the legal obligations of the CEO or System schools, for example, in relation to child protection legislation.

Volunteers:
A school also obtains personal information about volunteers who assist the school in its functions or conduct associated activities 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. In very limited situations, personal information held by a school may be disclosed to an organisation that assists in the school's fundraising, for example, the school's Parents and Friends Organisation or fete committees may receive limited, general information. School publications such as newsletters and magazines, which may include personal information, may be used for marketing purposes.

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

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

- other System school
- government departments
- the school's local parish and related Archdiocesan bodies

• medical practitioners
• people providing services to the school, including specialist visiting teachers, counsellors and sports coaches
• recipients of school publications, such as newsletters and magazines
• a parent
• anyone a parent authorises the school to disclose information to
• anyone to whom the school or the CEO are required to disclose the information to by law.

Sending and storing information overseas:
A school or the CEO may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, a school will not send personal information about an individual outside of Australia without:
• obtaining the consent of the individual (in some cases this consent will be implied)
• otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The school may also store personal information in the 'cloud' which may mean that it resides on servers which are situated outside of Australia. Schools must obtain assurances as to the use of such information when they have decided to store that information in the 'cloud.' Likewise, if the CEO decides to store personal information in the 'cloud' then the CEO must obtain such assurances.
Sensitive information will be used and disclosed only for the purpose for which it was provided or for a directly related secondary purpose, unless permissions are obtained, or the use or disclosure of the sensitive information is required by law. The handling of 'sensitive information' must be limited to a certain amount of people. Access to the storage of this information must also be limited whether it is in hard copy or electronically held. System schools and the CEO must develop a policy for access to sensitive information in its possession and outline the process of securing that information.

Management and Security of Personal Information

CEO and school staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals. Each school has in place steps to protect the personal information the school holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods, including locked storage of paper records and password access rights to applicable computerised records.

Access and Correction of Personal Information

Under the Commonwealth *Privacy Act* an individual has the right to obtain access to relevant personal information which the CEO or a school holds about them and to advise the CEO or the school of any perceived inaccuracy. A formal request must be made in writing to the CEO. Students will generally be able to access and update their personal information through their parents, but older students may seek access and permission to correct such information 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 CEO or a System school holds about you or your child, contact the school's Principal in writing. The school may require you to verify your identity, and specify the information you require. The school may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the school will advise the likely cost in advance. If the school or CEO cannot provide you with access to that information, they will provide

you with written notice explaining the reasons for refusal. Access may be restricted to protect the privacy of others, by reason of legal proceedings or because of child protection protocol.

Consent and rights of access to the personal information of students

The CEO 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. As mentioned above, parents may seek access to personal information held by a school or the CEO 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 the 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 warrants such action.

Enquiries and Complaints

For further information about the way the CEO or a System school manages the personal information it holds, or if an individual wishes to complain that they believe that the CEO or a System school has breached the Australian Privacy Principles, they must contact the school's principal, or the CEO. The CEO or the school will investigate any complaint in accordance with the CEO policy on Complaints, and will notify them of a decision in relation to their complaint as soon as is practicable after it has been made. Should an individual be dissatisfied with the response from a school or the CEO, they may then approach the Office of the Australian Information Commissioner (OAIC).

The CEO's contact details are:
Catholic Education Office
PO Box 3317
Manuka ACT 2603
Phone: (02)6234 5455
Email: reception@cg.catholic.edu.au

References

The Privacy Amendment (Enhancing Privacy Protection) Act 2012.
Further information about the Privacy Principles or the CEO's policies relating to privacy issues can be obtained from the Privacy commission's web site: www.privacy.gov.au

Forms
Standard Collection Notice for Schools
Employee Collection Notice Form

Approved by: Moira Najdecki

Issuing Service Area:	SALT
Implementation Date:	12 March 2014
Policy last updated:	February 2014
CEO Contact Officer:	Head of Human Resource Services
Trim Record Number:	