Citipointe Christian College

PRIVACY OF INFORMATION

Purpose
This policy outlines the Board's and the College's commitment to protecting the privacy of personal information that is collected by or provided to the College.

Policy
The policy ensures that the collection and usage of information for the management of College activities and for student welfare is in accordance with the Privacy Act 1988 Cwlth, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Australian Privacy Principles[1].

Classification of Information (extracted from http://www.oaic.gov.au/)
The Privacy Act 1988 (Privacy Act) regulates how personal information is handled.

The Privacy Act defines personal information as:
"…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.
Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person" and

Sensitive information is a type of personal information and includes information about:

- an individual's racial or ethnic origin
- health information
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- genetic information
- biometric information that is to be used for certain purposes
- biometric templates

5.1.1 Data Collection
Information is subdivided into 2 categories: solicited information and unsolicited information

The College collects and hold personal and sensitive information about:

- Students and parents and/or guardians (hereinafter referred to as "parents") before, during and after the course of a student's enrolment at the College;
- Job applicants, staff members, volunteers and contractors; and
- Other people who come into contact with the College

Solicited information is collected by way of forms filled out by parents or students, face-to-face meetings, at interviews and in telephone calls and is strictly for the purpose of providing schooling for the individual at the College.

Unsolicited information received by the school may be destroyed unless legal obligations necessitate otherwise.

[1] The Australian Privacy Principle is a set of harmonised principles which replaces both the Information Privacy Principles (IPPs) that applied to Australian Government agencies and the National Privacy Principles (NPPs) that applied to some private sector organisations. http://www.oaic.gov.au/

In some circumstances, the College 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. If the College should require additional personal or sensitive information of the individual from a third party, an authorised consent (i.e. via the parents or guardian) will be obtained unless an implicit authority is already given.

The College may also collect **unsolicited information** by way of video surveillance which is a practice implemented to assist the College with security and student protection matters. The surveillance cameras are installed on College buses and at strategic locations around the campus. All video footage is stored and managed privately by the assigned authorities and accessible for investigation purposes only in the event of an incident. This footage may be released to enforcement agencies if required subject to compliance with APP 6. The footage will be deleted or de-identified regularly to comply with APP 4.

The College is bound by the Australia Privacy Principles contained in the Commonwealth Privacy Act. The policy will be reviewed and updated in accordance with changes in legislative requirements and appropriateness to the College environment. The introduction of APPs (Australian Privacy Principles) do not negate the College's reasonable treatment of an employee record, where the treatment is directly related to a current or former employment relationship between College and employee.

In the current information age, we acknowledge that data may be collected via digital platforms such as Google Analytics, Wi-Fi connectivity, Internet of Things (IoT). The College may implement suitable and appropriate platforms to provide for the effective running of the College.

5.1.2 Data Use (APP 6)

Students and Parents: The collection of personal information is for the primary purpose of enabling the College to provide schooling for the student. This information will be used to address the needs of parents and the student throughout the period of enrolment at the College. The use of personal information for non-College related activities is strictly prohibited.

The secondary purpose for which the College 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 and medical wellbeing;
- Seeking donations and marketing for the College;
- To satisfy the College's legal obligations and allow the College to discharge its duty of care.

Full and frank disclosure of information sought is necessary to the formation of a contractual relationship between the College and parents.

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

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

- In administering the individual's employment or contract, as the case may be;
- For insurance purposes;
- Seeking funds and marketing the College;
- To satisfy the College's legal requirements.

N.B. The Privacy Act does not protect employment history from enquiry or disclosure.

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

Use of Information

a) College-based publications

College publications which include personal information, such as newsletters and magazines, will be provided to the school community.

b) Fundraising

The College regularly seeks funding support from its community to support its future growth and development with the intent to provide a high quality learning environment in which students and staff thrive. Consequently, personal information held by the College may be disclosed to an internal organisation such as the College's Cardo Foundation or alumni organisations that assist in the College's fundraising activities.

c) Marketing

Personal information provided by parents and staff will not be used in any form of direct marketing which is mutually exclusive to the core activity of the organisation. A separate consent will be sought for the identification of students prior to any marketing activity.

N.B. Parents and others may opt out of receiving funding and marketing information by writing to the College with the request.

5.1.3 Data Disclosure

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

- Another school;
- Government departments;
- Medical practitioners;
- People providing services to the College, including specialist visiting teachers and sports coaches;
- Recipients of College publications, such as newsletters and magazines;
- Parents; and
- Anyone you authorise the College to disclose information to.

Sending information overseas: The College will not send personal information outside Australia without first obtaining consent from the individual or the appropriate authorities (example: in the case of a minor, the consent may be from the parents or approved guardians) to comply with APP5.

For the purposes of storage of data external to Australia (e.g. by the Cloud) all reasonable steps will be taken to ensure security is safeguarded.

5.1.4 Data Quality

The College will aim to ensure that personal information that has been collected is accurate and up-to-date. To achieve this, the College will regularly review and update its database. An annual request for an update of personal information will be sent to all students and staff at the beginning of each academic year. Current changes can be requested by sending the updates via email to privacy@citipointe.qld.edu.au or in person at the College reception. Identity verification may be required to ascertain the validity of the request.

5.1.5 Data Security
The College will take all possible measures to ensure that the information that it holds within its systems is protected from unauthorised access. Security measures include password lock cabinets, key locked drawers and security password access for digitally stored information within the College mainframe.

The College may engage a third party service provider for storage of data (example: Microsoft Cloud). These third party servers may be located outside of Australia. Due diligence will be exercised in the process to identify and engage providers who are reputable to provide secure facilities. The College will endeavour to ensure that information is held securely with these providers.

5.1.6 Data Access
An individual who wants to access personal information collected by the College for schooling can do so by submitting a written request to the Compliance Office at privacy@citipointe.qld.edu.au The College will respond to the request within 10 working days. An administration charge may be levied for the extraction of the information.

The College will respond to the requestor with a written notification if the release of information is denied. The College has the prerogative to withhold the requested information if it has an unreasonable impact on the privacy of others, or may result in a breach of the College's duty of care to the student, or will have a negative impact on law enforcement.

5.1.7 Data Sensitivity
Sensitive data is information relating to a person's racial or ethnic origin, political opinions, religion, sexual preferences, health information, family or marital circumstances and/or criminal record. This sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless it is otherwise agreed, or the use or disclosure is allowed by law.

5.1.8 Privacy Breach
All breaches or suspected breaches of privacy are to be reported to the Principal and/or the IT Director or his delegate for immediate investigation and/or intervention. If the breach pertains to **eligible data**, the incident of the breach must be reported to the Privacy Commissioner within 30 days and to the police authority also, if it is of a criminal intent.

Eligible data includes personal information such as the following:

a. Medicare numbers, health care numbers
b. Financial account, salaries, leave details
c. Debit/Credit card details
d. Health condition e.g. mental illnesses, epilepsy, disability, HIV Aids
e. Addresses and whereabouts of persons under protection orders and such
f. Identity theft
g. Threat to emotional wellbeing, humiliation
h. Damage to reputation or relationship and
i. Legal liability
j. Photos and videos of school events
k. Complaints

The IT Director and/or his delegate will ascertain the severity of the breach and initiate a system intervention to stop the breach from furthering and contain the damage. The IT Director will update the Principal on the severity of the breach and the response taskforce may be convened to take appropriate action in response to the breach.

However, if the breach is not system related, the incident is to be brought to the attention of the Compliance Office and/or Principal. Likewise, an investigation will be initiated to ascertain the severity of the breach and the degree of harm to students, staff and/or their families. It is the prerogative of the Principal to activate the response taskforce to mitigate the risk that arises from the breach.

The Principal (or his delegate) is responsible to report the security and privacy breach to the College Board and the Governing Body, INC. The response team will collaborate on appropriate risk mitigation actions and preventative measures to prevent future occurrences.

The response team is responsible to

- take appropriate immediate action to contain the risk
- assess the severity of risk and establish the process for communicating to the affected staff, students, family and friends in the College community, if necessary.
- investigate, review and make recommendation on preventative measures to mitigate a recurrence. The College Executive will be responsible to implement the initiatives accordingly.

The Response team will include the following persons:

i. Principal and/or his delegate (Business Manager)
ii. IT Director
iii. Compliance Officer
iv. Heads of School
v. Registrar
vi. Development Director

The College IT department has a documented process to address data breaches should they occur. Refer to diagram (i).

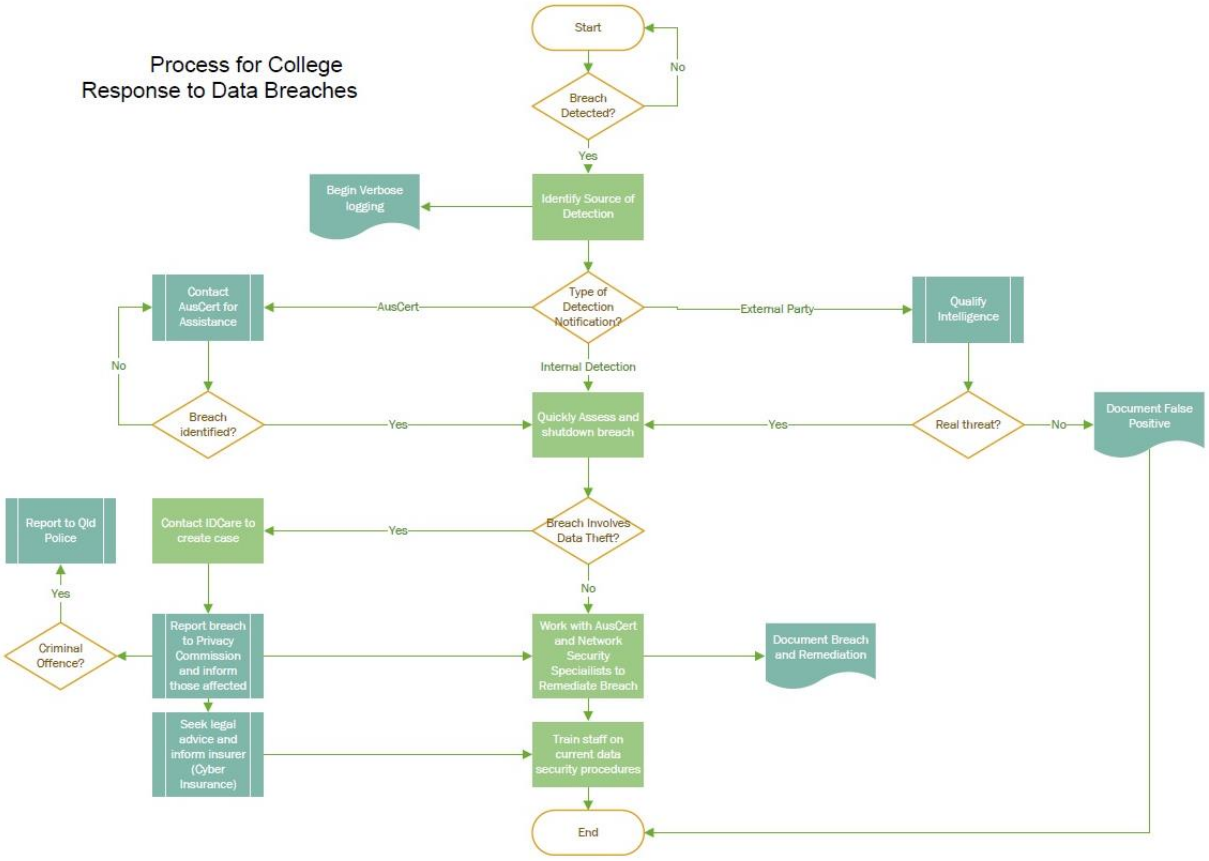

Diagram (i)

5.1.9 Complaint

a) **Internal Complaints**

The College will endeavour to keep all information current, accurate and secure. However, if there is inappropriate management of personal information, or if the individual appeals against the decision to withhold information, a complaint can be lodged in writing to the Principal and the matter will be addressed within 14 days after the complaint is received.

Any wilful misappropriation of private information (eligible or otherwise) will be investigated and the person(s) will be subject to the Principal's conduct review and if necessary referred to the appropriate authorities.

b) **External Complaints**

Should a person wish to lodge an external complaint with the Australian Privacy Commissioner, that procedure will be found on the Commission website.

Complaints are considered eligible private data and will be kept private and confidential. The data will be used strictly for addressing the matter of grief and resolution of conflict.

5.1.10 Policy Review

The policy will be reviewed every 2 years or as otherwise required.

Related Policies and Documents

- 4.3 Information Management and Security
- 7.1 Student Protection
- Acceptable Use guidelines
- Australian Privacy Principles 2014

Reference

- Privacy Act 1988
- Comlaw
- Australian Privacy Principles 2014
- Privacy Act 2017