HUNTER CHRISTIAN SCHOOL

PRIVACY AND DATA BREACH NOTIFICATION POLICY

Prepared by	Boyd Allen (Principal)
Date prepared	August 2011
Monitored by	Principal and Executive
Review by	Executive members
Date for review	With any serious data breach or changes to mandated requirements
Status	ACTIVE

Related Documents

Title	Author	Notes
HCS Procedure Data Breach Notification	HCS	Procedures for this policy
Privacy Amendment (Notifiable Data Breaches) Act 2017	Commonwealth	Legislative requirements
Privacy Act 1988	Commonwealth	Legislative requirements
Data breach response plan	Office of the Australian Information Commissioner	Sample procedure: https://www.oaic.gov.au/about-us/corporate-information/key-documents/data-breach-response-plan

Version History

Version	Date	Notes
1.0	August 2011	Initial Draft Document
1.1	March 2013	Minor revisions
1.2	Feb 2018	Incorporation of Data Breach Notification obligations (M. East – Principal)

Rationale
This statement outlines the School's policy on how the School uses and manages personal information provided to or collected by it. The school is bound by the National Privacy Principles contained in the Commonwealth Privacy Act. The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to School's operations and practices and to make sure it remains appropriate to the changing school environment.

Policy
The School look to manage all personal information with concurrent commitments to the respect of the individual, the responsibilities of staff to fulfil their functions, and the requirements of State.

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

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

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

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

Exception in relation to employee records: Under the Privacy Act the National 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.

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

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

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

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

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

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

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

Marketing and fundraising: The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to be a quality learning environment in which both pupils and staff thrive. Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising; for example, the School's Foundation or alumni organisation. Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

Disclosure of Personal Information

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

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

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

- Obtaining the consent of the individual (in some cases this consent will be implied); or
- Otherwise complying with the National Privacy Principles.

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

which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and Security of Personal Information – The School's staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals. The School has procedures to protect the personal information the School holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and pass worded access rights to computerised records.

Updating Personal Information – The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by the School by contacting the Receptionist of the School at any time. The National Privacy Principles require the School not to store personal information longer than necessary.

Right to Check – Under the Commonwealth Privacy Act, an individual has the right to obtain access to any personal information which the School hold about them and to advise the School of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Pupils will generally have access to their personal information through their Parents, but self-enrolling pupils and pupils 18 years or older may see access themselves. Generally the School will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's Parents. The School will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil. To make a request to access any information the School holds about you or your child, please contact the respective Principal in writing. The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Enquiries – If you would like further information about the way the School manages the personal information it holds, please contact the Principal.

Contractor/Volunteer Collection Notice

Contractors and Volunteers need to be aware of the need for our school to comply with the National Privacy Principles which were enacted at the end of 2001. The school has developed a detailed policy (Hunter Christian School Privacy Policy) to ensure it complies with these principles. As part of this policy we acknowledge the information that is required from various groups and individuals and kept on record at school. The following notice is provided to ensure that we have your consent for the use and disclosure where appropriate of this personal information.

1. In applying for this position you will be providing Hunter Christian School with personal information. We can be contacted at 51 Bull Street, Mayfield, (PO Box 10, HRMC, NSW 2310) on phone 0249672111, fax 0249676658 or email admin@hunterhchristian.nsw.edu.au.
2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.
3. You agree that we may store this information for up to seven years.
4. Access to this information may be available to you if you ask the school for it.

5. We will not disclose this information to a third party without your consent.
6. We are required to collect information regarding whether you are or have been subject of an Apprehended Violence Order and certain criminal offences under Child Protection law.
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties.

Employment Collection Notice

As an applicant for employment you need to be aware of the need for our school to comply with the National Privacy Principles which were enacted at the end of 2001. The school has developed a detailed policy (Hunter Christian School Privacy Policy) to ensure it complies with these principles. As part of this policy we acknowledge the information that is required from our applicants and kept on record at school. The following notice is provided to ensure that we have your consent for the use and disclosure where appropriate of this personal information.

1. In applying for this position you will be providing Hunter Christian School with personal information. We can be contacted at 51 Bull Street, Mayfield, (PO Box 10, HRMC, NSW 2310) on phone 0249672111, fax 0249676658 or email admin@hunterhchristian.nsw.edu.au.
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 agree that we may store this information for the purpose of the interview process only after which times it will be destroyed within two months unless it is further required for your employment.
4. You may seek access to your personal information that we hold about you if you are unsuccessful for the position. 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.
5. We ill not disclose this information to a third party without your consent.
6. We are required to conduct a criminal record chick and collect information regarding where you are or have been the subject of an AVO and certain criminal offences under Child Protection laws.
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why, that they can access that information if they wish and that the School does not usually disclose the information to third parties and that we may store their information for up to two months unless retained for the purpose of further employment.

Hunter Christian School Collection Notice

School members may be aware of the need for our school to comply with the National Privacy Principles which were enacted at the end of 2001. The School has developed a detailed policy (Hunter Christian School Privacy Policy) to ensure it complies with these principles. This policy defines how the School uses and manages personal information provided to or collected by it. The following notice is provided to ensure that we have your consent for the use and disclosure where appropriate of this personal information. The continuing enrolment of your child/ren will assume your consent to the following collection notice.

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

2. Some of the information we collect is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.
3. Certain laws governing or relating to the operation of schools require that certain information is collected. These include Public Health and Child Protection laws.
4. Health information about pupils is sensitive information within the terms of the National Privacy Principles under the Privacy Act. We ask you to provide medical reports about pupils from time to time.
5. 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, medical practitioners and people providing services to the School, including specialist visiting teachers, (sports) 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 collected from pupils is regularly disclosed to their parents or guardians. On occasions information such as academic and sporting achievements, pupil activities and other news is published in School newsletters, magazines and on our website.
8. Parents may seek access to personal information collected about them and their son/daughter by contacting the School. Pupils may also seek access to personal information about them. However, there will be occasions when access is denied. Such occasions would include where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the School's duty of care to the pupil, or where the pupils have proved information in confidence.
9. As you may know the School from time to time engages in fundraising activities. Information received from you may be used to make an appeal to you. It may also be disclosed to organisations that assist in the School's fundraising activities solely for that purpose. We will not disclose your personal information to third parties for their own marketing purposes without your consent.
10. We may include you contact details in a class list and School directory. If you do not agree to this you must advise us now.

If you provide the School with 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. They can access that information if they wish. The School does not usually disclose the information to third parties.

Data Breach Notification

On the 22 February 2018, the Notifiable Data Breach (NDB) Scheme is in force. The School is required to notify the Office of the Australian Information Commissioner (OAIC) and the affected individual(s), in the event of a notifiable data breach. This occurs in circumstances where:

- There is an unauthorised access or unauthorised disclosure of information and a responsible person would conclude that access or disclosure would be likely to result in serious harm to any of the individuals to whom it relates.
- Information is lost in circumstances where such unauthorised access or disclosure is likely to occur and a reasonable person would conclude that, assuming such access or disclosure did occur, it would be likely to result in serious harm to any individuals to who that information relates.

Where an eligible data breach is suspected or believed to have occurred, the School must:

- Carry out a risk assessment in the event that an eligible data breach is suspected.
- Prepare a statement of prescribed information regarding an eligible data breach that is believed to have occurred.
- Submit the statement to the OAIC
- Contact all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — Is serious harm still likely? — YES

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.