FINTONA
Girls' School

Privacy Statement

Purpose:

This statement outlines the policy of Fintona Girls' School's use and management of personal information provided or collected. The School is bound by the National Privacy Principles contained in the Commonwealth Privacy Act 2014 and the Health Privacy Principles contained in the Health Records Act 2002. The School may, from time to time, review and update its Privacy Policy to take new laws and technology into account and to make sure it remains appropriate to the changing school management and environment.

Policy:

Types of personal information kept by the School and how it is collected

The type of information the School collects and holds includes (but is not limited to) personal information, including 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 and
- other people who come into contact with the School.

Personal Information personally provided

The School will generally collect personal information about an individual by way of forms on Caremonkey filled out by parents or students, face-to-face meetings and interviews, and telephone calls. On occasion, people other than parents and students 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 employee records. 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.

How the School uses personal information provided

Students and Parents

In relation to personal information about students and parents, the School's primary purpose is to enable it to provide schooling for the student. This includes satisfying both the needs of parents and the needs of the student throughout the whole period they are enrolled at the School.

The purposes 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
- to look after pupils' educational, social and medical wellbeing
- to seek donations and marketing for the School
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

Where the 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 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:

- to administer the individual's employment or contract, as the case may be,
- for insurance purposes
- to seek 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 or those 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 which include personal information may be used for marketing purposes.

Disclosure of personal information by the School

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, sports coaches and camp facilities
- recipients of School publications, like newsletters and magazines;
- parents and

- anyone who individuals have authorised 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.

How the School treats 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, and health information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or for a directly related secondary purpose, unless otherwise agreed, 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 students and parents' personal information and the privacy of individuals.

The School has in place steps 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 Student Services or the Reception of the School at any time. The National Privacy Principles require the School to store personal information no longer than necessary.

You have the right to check what personal information the School holds about you

Under the Commonwealth Privacy Act, an individual has the right to obtain access to any personal information, which the School holds, about them and to advise the School of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Students will generally have access to their personal information through their parents, but older students may seek access themselves. To make a request to access any information the School holds about parents or students, contact the Business Manager in writing. The School will require parents to verify their identity and specify what information they require. The School may charge a fee to cover the cost of verifying an 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.

Consent and rights of access to the personal information of pupils

The School respects every parent's right to make decisions concerning their child's education. Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The 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 the School about them or their child by contacting the Business Manager in writing. 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.

The 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 so warrant.

Enquiries

If you would like further information about the way the School manages the personal information it holds, please contact the Business Manager.

Electronic Data Breach

Scope of the Policy:

For the purposes of this Policy, Data Breach is to be read as an Electronic Data Breach.

This Policy is to be used in the event of an electronic breach of data at Fintona Girls' School. In the event of a data breach, school personnel should follow procedures outlined in the Electronic Data Breach Response Protocol outlined below.

The following are examples of electronic data breaches which require the enactment of this Policy.

1. Loss of mobile devices of other School equipment containing personal information;
2. Cyber-attacks on the School systems, resulting in access to or theft of personal information;
3. Accidental transmission of personal information such as student's reports to unintended recipients via email;
4. Misuse of personal information of students or parents by School personnel;

Fintona Girls' School obligations imposed by the Australian Privacy Principles in the event of an electronic breach of data.

1. Take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the School's functions or activities that will ensure compliance with the APP; and
2. Take such steps that will enable the School to deal with inquiries or complaints about compliance with the APP;
3. Have a clearly expressed and up-to-date Privacy Policy about the School's management of personal information.

In the event of an electronic breach of data, Fintona Girls' School will follow the Privacy Breach Response Protocol as outlined below. It is important that appropriate records are kept of the response to the Privacy Breach, including the assessment of the risks associated with the Privacy Breach and the decisions made as to the appropriate action/actions to take in response to the Privacy Breach.

Phase 1. Contain the Privacy Breach and do a preliminary assessment

- School personnel who become aware of an electronic privacy breach must immediately notify the Principal and the Business Manager. This notification

should include, if known at this time, the time and date of the suspected privacy breach, the type of information involved, the cause and extent of the breach and who may be affected by it.

- The Principal and Business Manager must take any immediate steps to contain the Privacy Breach e.g. contact the IT department to shut down relevant systems or remove access to the systems.
- In containing the Privacy Breach, evidence should be preserved that may be valuable in determining the cause of the Privacy Breach.
- The Principal and the Business Manager must consider if there are any other steps that can be taken immediately to mitigate the harm an individual may suffer from the Privacy Breach.
- The Principal and the Business Manager must make a preliminary assessment of the risk level of the Privacy Breach. This will involve and analysis of the risks involved.
- The IT Manager must keep an electronic Log Book for High and Medium Risk Breaches. Information kept in the Log Book should consist of the following information;
  1. Date
  2. Timeframe of breach (approx.)
  3. Parties affected
  4. Cause of breach
  5. Who/when Principal and Business Manager notified
  6. Action taken
  7. Additional preventative measures taken

  Both the Principal and Business Manager should have access to the Log Book.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information, such as health information have been leaked externally. The Log Book should be activated by the IT Manager.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Privacy Breach, but there is an indication of a systemic problem in processes or procedures. The Log Book should be activated by the IT Manager
Low	A few names and school email addresses accidently disclosed to trusted third party, e.g. where email accidentally sent to wrong person. Near miss or potential event occurred. No identified loss, misuse or interference with personal information.

5. In the event that the Principal and or Business Manager receives multiple reports of Privacy Breaches of different databases, this may be part of related incident. The Principal and or Business Manager must consider upgrading the risk level if this situation arises.

6. Where a **high risk** incident is identified, the Principal and Business Manager must consider if the affected individuals should be notified immediately to mitigate the risk of serious harm to individuals.
7. The Principal and Business Manager must escalate **High Risk** and **Medium Risk** Privacy Breaches to the IT Manager.
8. If the Principal and Business Manager believe a **Low Risk** incident has occurred, he or she may determine that the IT Manager does not need to be alerted. They should then activate Phase 2 and 3.
9. If there should be media or school community attention as a result of the Privacy Breach, it should be escalated to the Principal and the Business Manager.
10. If appropriate, the Principal should pre-empt media interest by developing a communications or media response and strategy that manages public expectations.

Phase 2. Evaluate the risks associated with the Privacy Breach (Medium and High Risk Breaches)

1. The IT Manager is to take further steps i.e. those not identified in Phase 1) available to contain the Privacy Breach and mitigate harm to affected individuals.
2. The IT Manager is to work to evaluate the risks associated with the Privacy Breach by;
   a. Identifying the type of personal information involved in the Privacy Breach;
   b. Identifying the date, time, duration and location of the Privacy Breach;
   c. Establishing the extent of the Privacy Breach i.e. the number of individuals affected
   d. Establishing who the affected or possibly affected individuals are;
   e. Identifying what is the risk of harm to the individual/s and the extent of the likely harm e.g. what was the nature of the personal information involved;
   f. Establishing what the likely reoccurrence of the Privacy Breach is;
   g. Considering whether the Privacy Breach indicates a systemic problem with practices or procedures;
   h. Assessing the risk of harm to the School;
   i. Trying to establish the likely cause of the Privacy Breach;
3. The IT Manager should assess priorities and risks based on what is known.
4. The IT Manager does not need to consider a particular matter above if this will cause significant delays in proceeding to Phase 3.
5. The IT Manager should regularly update the Principal and the Business Manager regarding the incident status.

Phase 3. Consider Privacy Breach notification

6. Where appropriate, having regard for the seriousness of the Privacy Breach, the Principal and Business Manager must determine whether to notify the following stakeholders of the Breach;
   a. Affected individuals;
   b. Parents;
   c. The OIAC and/or;
   d. Other stakeholders e.g. if information which has been modified without authorisation is disclosed to another entity, that entity may need to be notified;
7. In general, if a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals, and their parents, if affected individuals are students, and the OAIC should be notified.

8. The Principal and Business Manager will facilitate ongoing discussion with the OAIC as required.

Phase 4. Take action to prevent future Privacy Breaches

9. The Principal and the Business Manager must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to phase 3. The cause of the Privacy Breach must be fully investigated.
10. The IT Manager must enter details of the Privacy Breach and response taken in the Privacy Breach Log Book. The IT Manager must, every year, review the Privacy Breach Log Book to identify reoccurring Privacy Breaches and notify the Principal and Business Manager.
11. The IT Manager must conduct post-breach reviews to assess the effectiveness of the School's response to the Privacy Breach and the effectiveness of the Privacy Breach Response Protocol.
12. The IT Manager must, if necessary, make suggestions to the Principal and Business Manager about appropriate changes to policies, procedures and staff training practices, including updating this Electronic Data Breach Policy Protocol.
13. The IT Manager must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Electronic Data Breach and conduct an audit to ensure the Plan is implemented.

Useful references and contacts

- OAIC's data breach notification; a guide to handling personal information security breaches
- OAIC's guide to developing a data breach response plan
- OAIC's website at www.oaic.gov.au
- National Computer Emergency Response Team; report Privacy Breaches to CERT via email info@cert.gov.au or phone 1300 172 499.
- Office of the Australian Information Commissioner; report Privacy Breaches to OAIC via email enquiries2oaic.gov.au or phone 1300363

Legislation:

Commonwealth Privacy Act 2014
Health Records Act 2002.

Responsibilities and Reviews

Responsibility of this Policy:	Principal
Implementation Date:	November 2017
Policy Review:	Annually
Review Year:	2020
Last Reviewed:	November 2017

Privacy Complaints

Procedure

Fintona Girls' School's policies and guidelines are intended to be up to date and be consistent with all relevant laws.

Employees and Contractors are expected to comply with all applicable policies and guidelines.

Various parts of the policies and guidelines require managers and staff to exercise discretion and the policies and guidelines are not intended to be applied in a legalistic or prescriptive manner.

These policies and guidelines may be varied by Fintona Girls' School from time to time, at its absolute discretion.

The policies and guidelines do not form part of an employee's contract of employment.

Purpose and Scope

Fintona Girls' School is subject to the Australian Privacy Legislation which contains Privacy Principals that the School must abide by when it collects, stores, uses and discloses personal information.

This purpose of this document is to provide a consistent and fair approach for handling complaints with respect to privacy of personal information. The procedure will apply if an individual considers that the School has acted in a manner that breached a Privacy Principal in respect of that individual.

Procedure Steps and Actions

1. A written complaint must be forwarded to the Business Manager within 6 months of the time the complainant first became aware of the alleged breach. The complaint must specify the details of the alleged breach.

2. The complaint may be made anonymously or using a pseudonym.

3. The Business Manager must make a determination on the complaint within 30 days of receipt of the complaint, and advise the complainant in writing.

4. If the Business Manager determines that there has been a breach of the Privacy Principals, he or she will, upon notification of the determination to the complainant, advise either the Principal or the Heads of School as applicable, of any action required to remedy the breach.

5. If the breach is capable of being rectified and is not rectified within 30 days of advice from the Business Manager, the Business Manager must inform the Principal.

6. The Business Manager will keep a record of all complaints. This will comprise a register and file records that will be securely stored in accordance with the current legislation.

Consequences if the Privacy Policy is deliberately breached

Disciplinary action, in accordance with the School's Performance and Conduct Management Policy, may be taken against any person who deliberately breaches the School's Privacy Policy.
Where the privacy breach has occurred due to a systemic failure, a review will be undertaken to ensure that the no further breaches will occur.