ABBOTSLEIGH

Privacy Policy

Policy number 3: Version 6

Rationale

Abbotsleigh is committed without reservation to delivering the highest quality education to its community. This quality is due in large part to the character of relationships and efficacy of communication between students, parents and the School. The nature of this communication is informed by the complexities of education and requires that the School be sufficiently informed to exercise sound judgement and offer constructive guidance. Being so informed requires the School to collect, use and disclose the Personal Information of students and parents.

The School regards its partnership with families as fundamentally important and will communicate with parents and students regularly on matters relating to teaching and learning, attendance, School activities and discipline. When making judgements about how, when, what and to whom to communicate, the School takes account of its responsibilities in relation to parents and students respectively, matters of privacy, the sensitivity of the information, its general duty of care and the wellbeing of those involved.

This Policy has been prepared to meet the requirements of the Australian Privacy Principles contained in the Commonwealth Privacy Act 1988 (Privacy Act). In relation to health records Abbotsleigh is also bound by the New South Wales Health Privacy Principles contained in the Health Records and Information Privacy Act 2002. The School has additional relevant obligations under the Workplace Surveillance Act 2005 and the Surveillance Devices Act 2007.

1. Policy objectives

This policy has been created to explain:

a) What Personal Information (Privacy Act, Section 6) Abbotsleigh collects and how it collects it;

b) How Abbotsleigh uses the Personal Information; and,

c) How Abbotsleigh might disclose the Personal Information.

2. Policy implementation and responsibilities

2.1 Compliance with the Australian Privacy Principles and other relevant privacy codes

2.1.1 Abbotsleigh will manage Personal Information in an open and transparent way in accordance with this Policy. Abbotsleigh will take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its functions or activities that will ensure that it complies with the Australian Privacy Principles and other relevant privacy codes and will enable it to deal with inquiries or complaints from individuals about the School's compliance with the Australian Privacy Principles or such a code.

2.2 Collection of Personal Information

2.2.1 Abbotsleigh will endeavour to collect only information which is reasonably necessary for its functions or activities.

2.2.2 The type of information that Abbotsleigh collects and holds includes (but is not limited to) Personal Information including health and other sensitive information (Privacy Act, Section 6) about:

a) Pupils, prospective pupils and parents and/or guardians (parents) before, during and after the course of a pupil's enrolment at the School;

b) Employees, job applicants, volunteers and contractors; and,

c) Other people who come into contact with the School (including alumni).

2.2.3 Abbotsleigh will generally collect this information by way of digital or hard copy collection documents, other online applications, TAS, the Abbotsleigh website, AbbNet, face-to-face meetings, events and interviews, and telephone calls. In some circumstances Abbotsleigh 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.

2.3 Use of Personal Information

2.3.1 Generally, Abbotsleigh may use Personal Information for the following purposes:

a) To keep parents informed about matters related to their child's schooling including teaching and learning, attendance, School activities and discipline through personal communication including academic reports and parent teacher interviews;

b) To improve the experience of pupils, educators and the School community

c) To perform day-to-day administration;

d) To look after pupils' educational, social and medical wellbeing;

e) To assess eligibility for scholarship and/or financial support purposes;

f) To seek donations and conduct marketing activities for the School;

g) To celebrate individual achievement in academic, sport, music or other pursuit;

h) To administer an individual's employment or contract;

i) For insurance purposes; and,

j) To satisfy the School's legal obligations, for example, in relation to child protection legislation, and allow the School to discharge its duty of care.

2.4 Disclosure of Personal Information

2.4.1 The people and organisations to whom Abbotsleigh may disclose Personal Information held about an individual include:

a) The Abbotsleigh Foundation (refer to the Abbotsleigh website for a copy of the Foundation's Privacy Policy).

b) Another school;

c) Government departments;

d) Medical practitioners;

e) People providing services to the School, including specialist visiting teachers, counsellors, legal advisors and sports coaches;

f) Providers of learning and assessment tools;

g) Assessment and educational bodies

h) Recipients of School publications, like newsletters and magazines (excluding sensitive information)

i) Parents;

j) People whom the relevant pupil, parents, job applicant, volunteer, contractor or other person authorise the School to disclose information to; and,

k) Other entities as required by law or where disclosure is necessary to prevent a threat to life, health or safety.

2.4.2 Abbotsleigh will only disclose information to a person or organisation after taking reasonable steps to satisfy itself that the person or organisation: a) has adopted information handling and storage

protocols complying with the Australian Privacy Principles; and b) will keep that disclosed information confidential.

2.4.3 Abbotsleigh does not sell or license Personal Information to any person or organisation.

2.4.4 Abbotsleigh may disclose Personal Information (including sensitive information) to an overseas recipient, for instance, to facilitate an international exchange or overseas field trip. However, Abbotsleigh will not send Personal Information about an individual to an overseas recipient: a) without expressly informing the individual that such a disclosure may occur; or b) unless the School reasonably believes the disclosure is necessary to prevent a serious threat to the life, health or safety of any individual or to public health or safety; or c) where a permitted general situation (Privacy Act, Section 16A) exists.

2.4.5 Abbotsleigh 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. Limited Personal Information may also be provided to these service providers to enable them to authenticate users. This Personal Information may be stored in the 'cloud' which means it may reside on a cloud service provider's server situated outside Australia.

2.5 Storage, retention and security of Personal Information

2.5.1 Abbotsleigh has in place steps to safeguard its information management systems and protect the Personal Information it holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records, secured servers and appropriate user access controls to computerised records.

2.5.2 Abbotsleigh retains information, including Personal Information, provided or collected before, during and after attendance, or other interaction with the School, for purposes of reasonable use as detailed at 2.3.1.

2.6 Updating Personal Information

2.6.1 Abbotsleigh endeavours to ensure that the Personal Information it holds is accurate, complete and up-to-date. Any person who believes the information Abbotsleigh holds about them requires changing or is out of date should contact the Head of Abbotsleigh.

2.6.2 If Abbotsleigh is satisfied that Personal Information about an individual is inaccurate, incomplete, not up-to-date, irrelevant or misleading and an individual requests Abbotsleigh to correct the information, Abbotsleigh will take reasonable steps to correct the information, having regard to the purpose for which it is held.

2.7 Right to check Personal Information

2.7.1 Under the Australian Privacy Principles, any person may be able to obtain a copy of the Personal Information Abbotsleigh holds about them. The Australian Privacy Principles provide some exceptions in this regard.

2.7.2 To make a request to access this information, a person should write to the Head of Abbotsleigh. Abbotsleigh may require verification of identity and specification of the information required, and may charge a fee to recover the cost of verifying the application and locating, retrieving, reviewing and copying any material requested. If this is the case, Abbotsleigh will advise the likely cost in advance.

2.7.3 Pupils will generally have access to their Personal Information through their parents, but older pupils may seek access themselves (as set out in the following section).

2.8 Consent to collection, use and disclosure of Personal Information

2.8.1 Generally, Abbotsleigh will refer requests for consent to collect, use and disclose Personal Information pertaining to a pupil or her parents to the parents.

2.8.2 In circumstances where a pupil is aged below 15 years and Abbotsleigh considers it appropriate in accordance with the Australian Privacy Principles, Abbotsleigh will treat consent to collect, use and disclose Personal Information given by parents as consent given on behalf of the pupil, and notice to parents will act as notice given to the pupil.

2.8.3 In circumstances where the pupil is aged 15 years or above and Abbotsleigh considers it appropriate in accordance with the Australian Privacy Principles, Abbotsleigh will seek consent to collect, use and disclose Personal Information from both the parents and the pupil and issue relevant notices to both the parent and the pupil.

2.9 Access to Personal Information held by Abbotsleigh

2.9.1 Circumstances may arise where parents and/or pupils seek access to Personal Information Abbotsleigh holds in a manner which differs from the School's regular pattern of communication. When making judgements concerning access in such cases, the School takes account of its responsibilities in relation to parents and students respectively, the Australian Privacy Principles, the sensitivity of the information, its general duty of care and the wellbeing of those involved.

2.9.2 Requests for access to Personal Information the School holds are addressed to the Head of Abbotsleigh in writing.

2.10 Notification of Eligible Data Breaches

2.10.1 In the event Abbotsleigh becomes aware of or has reasonable grounds to suspect, an unauthorised access to, modification or disclosure of, or other interference with, misuse or loss of control of Personal Information held by the School, it will cause an investigation to occur in accordance with Abbotsleigh's Data Breach Response Plan (refer Attachment).

2.10.2 In the event investigations at 2.10.1 identify an Eligible Data Breach, the School will notify persons affected by the breach and the Office of the Australian Information Commissioner in conformance with the Privacy Act.

2.11 Further information

2.11.1 Any person who requires further information about the way Abbotsleigh manages the Personal Information it holds or wishes to complain that they believe the School has breached the Australian Privacy Principles should contact the Director of Compliance.

2.11.2 Abbotsleigh will investigate any complaint and advise the complainant of any decision arising from the results of the investigation as soon as practicable after a decision has been made.

2.12 Exception in relation to employee records

2.12.1 Under the Privacy Act and the Health Records Act, 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 Abbotsleigh's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between Abbotsleigh and employee.

3. Related documentation

- Staff Code of Conduct
- Security Policy
- Critical Incident Policy
- Australian Privacy Principles
- Privacy Act and associated legislation
- Academic Care Policy

4. Information management

4.1 Ratification

This policy has been approved by the Council of Abbotsleigh.

4.2 Publishing this policy

Student Diary	No	Council	Yes
Staff Handbook	No	The Shuttle	No
AbbNet	Yes	Other	NA

4.3 Communicating this policy

Audience	Communicated by	Communication pathway
All staff, Council, parents and students	Head of Abbotsleigh, Heads of School and Council	As appropriate

4.4 Sharing this policy

A decision to share this document with an outside agent is made in consultation with the relevant Executive member. A sharing arrangement is subject to the following conditions: Abbotsleigh must be attributed as the source in any reference or derivative; commercial use is not permitted. Contact the Director of Compliance prior to sharing this document.

4.5 Policy history

4.5.1 Version 1, 2003.
4.5.2 Version 2, 2007: Substantial change to text
4.5.3 Version 3, 2010: Revised by GRCC to bring format in line with general policy format
4.5.4 Version 4, 2011: Revised by GRCC including extensions to use of information and minor amendments to disclosure.
4.5.5 Version 5, 2015:
4.5.6 Version 5.1: insert 2.4.1 a)
4.5.7 Version 6, 2018

4.6 Policy review

This policy is due for review in 2022.

Data Breach Response Plan

Introduction

1. This Data Breach Response Plan (DBRP) sets out procedures and lines of authority for Abbotsleigh (the School) in the event the School experiences a data breach or suspects a data breach has occurred.
2. A data breach occurs when Personal Information held by Abbotsleigh is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference.[1]
3. The DBRP will enable Abbotsleigh to contain, assess and respond to data breaches in a timely manner, determine whether a breach is serious and help mitigate potential harm to individuals affected.
4. An eligible data breach must be notified to the individual(s) involved and the Office of the Australian Information Commissioner (OAIC)

Responding to a data breach

Data breach occurs or suspected

Breach detected, or breach suspicion formed by employee or Abbotsleigh otherwise alerted

Response from Abbotsleigh Employee

Employee notes time and date of the breach, type of Personal Information involved and cause and extent of the suspected breach.

Employee advises their Senior Manager and Director of Compliance immediately.

Action by Senior Manager and Director Compliance

The Senior Manager and Director Compliance will investigate and assess whether a data breach has occurred.

A minor data breach may be able to be dealt with by the Senior Manager and Director Compliance. A serious data breach must be escalated to DBRT

Minor data breach

Where a minor data breach is dealt with at the Senior Manager/Director of Compliance level, the Director Compliance will create a record containing the following details:

- The date and time of the incident
- Action taken to contain and address the breach
- The outcome of the action
- A statement that, in the Manager's and Director's view, no further action is required
- Signoff from the Head that no further action is required.

Serious data breach

The Director Compliance will convene the DBRT

Non-eligible data breach

The DBRT will undertake steps in line with the response Plan

Eligible data breach

Where an eligible data breach has occurred, it is reportable to the individual(s) concerned and the OAIC

[1] OAIC - Data breach notification guide: A guide to handling Personal Information security breaches, August 2014

Distinguishing minor and serious data breaches

5. The relevant Senior Manager and the Director of Compliance will exercise discretion in determining whether a data breach is minor and can be dealt with without convening DBRT.

6. For example, an employee may send an email containing a student's Personal Information to an unintended recipient. If the email can be recalled successfully, it is unlikely to be necessary to refer the matter to DBRT.

7. In exercising discretion, the Senior Manager and Director Compliance should consider the following:
   a) Are multiple individuals affected by the breach?
   b) Is there a real or potential risk of serious harm to the affected individuals?
   c) Does the breach or suspected breach indicate a systemic problem with Abbotsleigh processes or procedures?
   d) Could the breach prompt media or stakeholder attention?
   e) Does the breach involve disclosure of Personal Information, particularly of a class likely to cause an individual harm if disclosed (refer also 16 b))?

8. If the answer to any question is yes, the breach may be an eligible data breach and notifiable to OAIC and the matter must be referred to DBRT.

The Data Breach Response Team

9. Members of the DBRT are:
   - The Head
   - The relevant Head of School
   - The Director Technology
   - The Director Compliance
   - The Bursar

10. Data breaches will be dealt with on a case by case basis undertaking an assessment of risk and relying on that assessment to determine an appropriate course of action.

11. The DBRT response to a suspected eligible data breach is comprised of four steps:
    - Step 1: Contain the breach and conduct a preliminary assessment
    - Step 2: Assess the risks associated with the breach against AOIC criteria to determine if it is an eligible data breach
    - Step 3: Notify as necessary
    - Step 4: Prevent further breaches

12. Steps 1 – 3 should occur simultaneously or in quick succession.

Responding to data breaches: four key steps[2]

Step 1 – Contain breach and conduct a preliminary assessment

13. Once a breach has been identified, immediate containment action must be taken. For example, stop the unauthorised practice, recover the records or shut down the system that was breached.

14. The DBRT must, as soon as practicable, appoint a person to lead the initial investigation to verify that a breach has occurred. The person must be suitably qualified and have sufficient authority to conduct the initial investigation.

Step 2 – Assess whether the data breach is an eligible data breach[3]

15. If a breach is confirmed at Step 1, or there is reason to suspect a breach has occurred, DBRT must conduct an assessment to determine that an eligible data breach has or, on the balance of probabilities is likely to have occurred.[4] A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the breach relates. The DBRT must take all reasonable steps to complete the assessment within 30 calendar days after Abbotsleigh became aware of the grounds (or information) that caused it to suspect an eligible data breach.

16. The assessment will seek to determine;
    a) That there has been unauthorised access to, disclosure of or a loss of Personal Information Abbotsleigh holds about an individual or individuals

        - Unauthorised access occurs whenever Personal Information is accessed by someone without authorisation. This includes unauthorised access by an employee as well as by an external party (hacking).
        - For example, an employee browses the payroll records of colleagues.

    b) That a risk of serious harm to one or more individuals affected by the breach is likely
        - Decision made from the standpoint of a reasonable, well-informed school administrator based on information immediately available or following reasonable inquiries or assessment
        - Likely means the risk of serious harm is more probable than not (rather than possible)
        - Serious harm may include serious physical, psychological, emotional, financial or reputational harm.[5]
        - Some types of Personal Information are more likely to cause an individual serious harm if compromised: Sensitive Information[6]; documents used for identity fraud (Medicare card, driver licence, passport); financial information; multiple items of Personal Information
        - The circumstances of the data breach should be taken into account[7]

    c) The extent to which Abbotsleigh has been able to prevent the likely risk of serious harm by remedial action

---

[2] Ibid, pp 13
[3] OAIC – Assessing an eligible data breach, September 2017
[4] OAIC – Identifying eligible data breaches, May 2017
[5] Ibid, pp 3-4
[6] Refer s 6 (1) of the Privacy Act for categories of Personal Information covered by the definition of sensitive information
[7] OAIC – Identifying eligible data breaches, May 2017, pp 4-5

- If Abbotsleigh takes remedial action to prevent harm occurring for any individuals whose Personal Information is involved in the breach, and as a result of this action the data breach is not likely to result in serious harm, it is not necessary to make any notifications.
- For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to or disclosure of the information.

17. If the assessment concludes there has been a data breach which is likely to result in serious harm to the individuals concerned and the likely risk of serious harm has not been mitigated by remedial action, an eligible data breach has occurred, and persons affected and the OAIC must be notified.

18. The Director Compliance will compile and retain a record of DBRT's processes including details of:
    a) The date, time and nature of the breach including a description of causality
    b) Person's affected by the breach
    c) The risks of harm and judgements as to the likelihood of harm and seriousness of harm
    d) The outcome of the assessment including whether the breach is determined to be an eligible data breach and notifiable to individuals affected and the OAIC
    e) The steps taken to reduce the risk of a similar breach occurring in future.

Step 3 – Notify as necessary

19. Providing notification about low risk breaches may cause undue anxiety and desensitise individuals to notice.

20. If DBRT determines an eligible data breach has occurred, it must arrange to notify affected individuals as soon as practicable. Prompt notification can assist individuals mitigate potential damage by prompting them to take steps to protect themselves.

21. A data breach statement to individuals must include:[8]
    a) Contact details of relevant Abbotsleigh employees
    b) A description of the data breach
    c) The kinds of information involved in the data breach
    d) Steps Abbotsleigh recommends individuals take in response to the data breach.

22. The data breach statement must be provided to the OAIC using either the online form available at the OAIC website or by email, including a copy of data breach statement as an attachment, to enquiries@oaic.gov.au

[8] OAIC – What to include in an eligible data breach statement, September 2017