Privacy and Data Breach Policy

This Privacy and Data Breach Policy sets out how St Paul's Anglican Grammar School manages personal information provided to or collected by it.

The School is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act. In relation to health records, the School is also bound by the Victorian Health Privacy Principles which are contained in the *Health Records and Information Privacy Act 2002* (Health Records Act).

The School may, from time to time, review and update this Privacy and Data Breach Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

What kinds of personal information does the School collect and how does the School collect it?

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

- students and parents and/or guardians ('Parents') 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 you provide:

The School will generally collect personal information held about an individual by way of forms filled out by Parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions 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 and the Victorian Health Records and Information Privacy Act 2002, 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 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 will the School use the personal information you provide?

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 by you, or to which you have consented.

Students and Parents:

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

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the School;
- looking after students' educational, social and medical wellbeing;
- seeking donations and marketing for the School; and
- 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 student or Parent, if the information requested is not provided, the School 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, 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:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking donations and marketing for the School; and
- 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 the Alumni Association, 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 provide a quality learning environment in which both students and staff thrive. Personal information held by the School may be disclosed to organisations that assist in the School's fundraising, for example, the School's Foundation or Alumni Association or, on occasions, external fundraising organisations. 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.

Who might the School disclose personal information to?

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, counsellors and sports coaches;
- recipients of School publications, such as newsletters and magazines;
- Parents;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required to disclose the information by law.

Sending information overseas:
The School may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers which are situated outside Australia or to facilitate a school exchange. However, 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 Australian Privacy Principles or other applicable privacy legislation.

How does the School treat 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, philosophical beliefs, sexual orientation or practices or criminal record, and also personal information; health information and biometric 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 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, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

Access and correction of personal information

Under the Commonwealth Privacy Act and the Health Records 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. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves. There are some exceptions to these rights set out in the applicable legislation. To make a request to access any personal information the School holds about you or your child, please contact the School 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. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of students

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. As mentioned above, parents may seek access to personal information held by the School about them or their child by contacting the School Principal. 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 student.

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 warranted.

Enquiries and complaints

If you would like further information about the way the School manages the personal information it holds, or wish to complain that you believe that the School has breached the Australian Privacy Principles please contact the School Principal. The School will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

Version 2

Date Reviewed: May 2022
Reviewed By: Executive
Date to be Reviewed: May 2023

Privacy and Data Breach Policy Annexures

Rationale

The St Paul's Anglican Grammar School Privacy and Data Breach Policy sets out how the school will manage information provided to or collected by it as well as access to and correction of personal information. St Paul's Anglican Grammar School is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act. In addition, St Paul's Anglican Grammar School is bound by other legislation relating to information such as health records.

The School will ensure that any data breaches are investigated promptly and all eligible data breaches (EDB) are reported to the Information Commissioner as well as fulfilling our obligation to notify affected individuals. Following assessment of a data breach a review of the situation that led to the breach will be undertaken to avoid as much as possible a repeat of this. The process for responding to a data breach is outlined in these annexures to the privacy policy.

Privacy and Data Breach Policy Annexure 1

Privacy/Data Breach Risk Assessment Factors

Consider who the personal information is about	
Who is affected by the breach?	Are students, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.
Consider the kind or kinds of personal information involved	
Does the type of personal information create a greater risk of harm?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) may pose a greater risk of harm to the affected individual(s) if compromised. A combination of personal information may also pose a greater risk of harm.
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	For example, a disclosure of a list of the names of some students who attend the school may not give rise to significant risk. However, the same information about students who have attended the School Counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and addresses of students or parents would also create more significant risks.
Who has gained unauthorised access to the affected information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher at another school gains unauthorised access to a student's name, address and grades without malicious intent (e.g. if the information is accidentally emailed to the teacher), the risk of serious harm to the student may be unlikely.

Have there been other breaches that could have a cumulative effect?	A number of minor, unrelated breaches that might not, by themselves, create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches is considered. This could involve incremental breaches of the same school database, or known breaches from multiple different sources (e.g., multiple schools or multiple data points within the one school).
How could the personal information be used?	Consider the purposes for which the information could be used. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual and social or workplace bullying)? For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents. What is the risk of harm to the individual if the compromised information can be easily combined with other compromised or publicly available information?
Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	What is the risk of further repeat access, use or disclosure, including via mass media or online?
Is there evidence of intention to steal the personal information?	For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in way that renders it unusable if breached. If so, the risk of harm to the individual may be lessened.
What was the source of the breach?	For example, was it external or internal? Was it malicious or unintentional? Did it involve malicious behaviour or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information lost or stolen? Where the breach is unintentional or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.
Has the personal information been recovered?	For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?
What steps have already been taken to mitigate the harm?	Has the school fully assessed and contained the breach by, for example, replacing comprised security measures such as passwords? Are further steps required? This may include notification to affected individuals.

Is this a systemic problem or an isolated incident?	When identifying the source of the breach, it is important to note whether similar breaches have occurred in the past. If so, there may be a systemic problem with system security, or there may be more information affected than first thought, potentially heightening the risk.
How many individuals are affected by the breach?	If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response must be proportionate. Although it is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.
Assess the risk of harm to the affected individuals	
Who is the information about?	Some individuals are more vulnerable and less able to take steps to protect themselves (e.g. younger students, students with disabilities/special needs, vulnerable families/parents).
What kind or kinds of information is involved?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) or a combination of personal information may pose a greater risk of harm to the affected individual(s) if compromised.
How sensitive is the information?	The sensitivity of the information may arise due to the kind of information involved, or it may arise due to the context of the information involved. For example, a list of the names of some students who attend the school may not be sensitive information. However, the same information about students who have attended the School counsellor or students with disabilities would pose a greater risk to individuals.
Is the information in a form that is intelligible to an ordinary person?	Examples of information that may not be intelligible to an ordinary person, depending on the circumstances may include: (i) encrypted electronic information; (ii) information that the school could likely use to identify an individual, but that other people likely could not (such as a student number that only the school uses – this should be contrasted to a student number that is used on public documents); and (iii) information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).
If the information is not in a form that is intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?	For example, encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the breach. Even where none of these concerns apply, the school may need to consider the likelihood of the encryption algorithm being broken in the long term.
Is the information protected by one or more security measures?	For example, are the systems on which the information is stored protected by intrusion detection and prevention systems, which identified the attack and stopped the attacker from accessing any information or copying the information?

If the information is protected by one or more security measures, what is the likelihood that any of those security measures could be overcome?	For example, could an attacker have overcome network security measures protecting personal information stored on the network?
What persons (or kind of persons) have obtained or could obtain the information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a student's information without malicious intent, the risk of serious harm may be unlikely.
What is the nature of the harm that could result from the breach?	Examples include identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of business or employment opportunities, humiliation, damage to reputation or relationships, or workplace or social bullying or marginalisation. For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents.
In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?	Examples of steps that may remediate the serious harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorised practice, recovering records subject to unauthorised access or disclosure or loss, shutting down a system that was subject to unauthorised access or disclosure, or remotely erasing the memory of a lost or stolen device. Considerations about how quickly these steps are taken or the extent to which the steps taken are remediating harm will vary depending on the circumstances.
Any other relevant matters?	The nature of other matters that may be relevant will vary depending on the circumstances of the School and the Data Breach.
Assess the risk of other harms	
What other possible harms could result from the breach, including harms to the school ?	Examples include loss of public trust in the School, damage to reputation, loss of assets (e.g. stolen laptops), financial exposure (e.g., if bank account details are compromised), regulatory penalties (e.g., for breaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.

Privacy and Data Breach Policy Annexure 2

Privacy Breach Response Protocol

Introduction

This protocol sets out the procedure to manage the School's response to the actual or suspected misuse, interference, loss, or unauthorised access, modification or disclosure of personal information (**Privacy Breach**). It is intended to enable the school to contain, assess and respond to a Privacy Breach.

Response protocol

In the event of a Privacy Breach, the school must adhere to the following four phase process (as described in the Office of the Australian Information Commissioner's (**OAIC**) guide *Data breach notification: a guide to handling personal information security breaches*). Phases 1 – 3 should occur in quick succession and may occur simultaneously.

It is important that appropriate records are kept of the response to the Privacy Breach, including the assessments of the risks associated with the Privacy Breach and decisions made as to the appropriate action/s to take in response to the Privacy Breach.

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

1. The school staff member who becomes aware of the Privacy Breach must immediately notify the IT Help Desk. This notification should include (if known at this stage) the time and date the suspected Privacy Breach was discovered, the type of personal information involved, the cause and extent of the Privacy Breach, and who may be affected by the Privacy Breach.
2. IT Staff will inform the Incident Deputy (Director of Information Services) who will make an initial assessment and contact the Deputy Principal (Incident Lead).
3. The Incident Lead or Delegate must take any immediately available steps to contain the Privacy Breach (e.g., direct the IT department, if practicable, to shut down relevant systems or remove access to the systems).
4. In containing the Privacy Breach, evidence should be preserved that may be valuable in determining the cause of the Privacy Breach. This is particularly relevant if there is a Privacy Breach involving information security.
5. The Incident Lead or Delegate 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.
6. The Incident Lead or Delegate must make a preliminary assessment of the risk level of the Privacy Breach. This will involve an analysis of the risks involved. (See Annexure 1)
7. In the event that the Incident Lead or Delegate receives multiple reports of Privacy Breaches of different datasets, this may be part of a related incident and the Principal or Delegate must consider upgrading the risk level if this situation arises.
8. Where a High Risk incident is identified, the Incident Lead or Delegate must consider if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals.
9. The Incident Lead or Delegate must escalate High Risk and Medium Risk Privacy Breaches to the Response Team (whose details are set out at the end of this protocol).
10. If the Incident Lead or Delegate believes a Low Risk Privacy Breach has occurred, he or she may determine that the Response Team does not need to be convened. In this case, he or she must undertake Phases 2 and 3 below.
11. If there could be media or stakeholder attention as a result of the Privacy Breach, it must be escalated to the response team.
12. If appropriate, the Response Team 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

1. The Response Team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Privacy Breach and mitigate harm to affected individuals.
2. The Response Team 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 (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 and other organisations including the Anglican Diocese of Gippsland and Ecumenical Schools Australia
    i. establishing the likely cause of the Privacy Breach.
3. The Response Team should assess priorities and risks based on what is known.
4. The Response Team does not need to consider a particular matter above if this will cause significant delay in proceeding to Phase 3.
5. The Response Team should regularly update each other and other relevant stakeholders regarding incident status.

Phase 3. Consider Privacy Breach notifications

1. Where appropriate, having regard to the seriousness of the Privacy Breach (based on the evaluation above), the Response Team must determine whether to notify the following stakeholders of the Privacy Breach:
    a. affected individuals;
    b. parents;
    c. the OAIC (Office of the Australian Information Commissioner); 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).
2. In general, if a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals (and their parents if the affected individuals are students) and the OAIC should be notified.
3. The response team will facilitate ongoing discussion with the OAIC as required.

Phase 4. Take action to prevent future Privacy Breaches

1. The response team 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.
2. The Incident Lead or Delegate must enter details of the Privacy Breach and response taken into a Privacy Breach log. The Incident Lead must, every year, review the Privacy Breach log to identify any reoccurring Privacy Breaches.
3. The Incident Lead must conduct a post-breach review to assess the effectiveness of the School's response to the Privacy Breach and the effectiveness of the Privacy Breach Response Protocol.
4. The Incident Lead must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Privacy Breach Response Protocol.
5. The Incident Lead must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Privacy Breach and conduct an audit to ensure the plan is implemented.

Response Team

The Response Team would usually consist of the Deputy Principal (*Incident Lead*), the Director of Information Services (*Incident Deputy*), Director of Development (*Communications Lead*), Executive Assistant (*Compliance Lead*) and, when required, the Business Manager (*Financial Lead*) and the IT Network Manager (*IT Support Lead*).

The Incident Lead or Delegate would generally oversight the response process and provide reports to the group as well as maintaining a Register for Privacy Breaches.

The Incident Deputy would usually conduct the investigation into an alleged Breach and make a recommendation based on the findings to the Incident Lead.

The IT Support Lead would be responsible for providing information requested for the investigation, where required, and actioning the directions of the Incident Lead, Incident Deputy or Delegate in response to a Breach.

Other key staff members would become part of the response Team as needed.

DBRT Contingency plan

In the event whereby a DBRT role cannot be performed due to being absent or other reasons, the following contingency will take place:

Incident Lead	**Incident Deputy** will assume the role of **Incident Lead**
Incident Deputy	**IT Support Lead** will assume the role of **Incident Deputy**
Communications Lead	**Marketing Team member** will assume the role of **Communications Lead**
Financial Lead	**Accountant** will assume the role of **Financial Lead**
IT Support Lead	**IT Support Team member** will assume the role of **IT Support Lead**
Compliance Lead	**Assistant to Deputy Principal** will assume the role of **Compliance Lead**

Privacy and Data Breach Policy Annexure 3

Data Breach Response Plan

Introduction

This plan sets out the procedure which will be used to manage the School's response to an actual or suspected privacy or data breach.

Response plan

In the event of a Data Breach, the school must adhere to the four phase process set out below (as described in the Office of the Australian Information Commissioner's (**OAIC**) *Notifiable Data Breaches scheme: Resources for agencies and organisations*. It is important that appropriate records and any evidence are kept of the Data Breach and the response. Legal advice should also be sought, if necessary.

Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The staff member who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the IT Help Desk. The Incident Deputy (or Delegate) will ensure immediately all available steps are to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence must be preserved that may be valuable in determining its cause.
3. The Incident Deputy will nominate an officer to make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally 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 of personal information.

4. Where a High-Risk incident is identified, the Incident Deputy will inform the Incident Lead who must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. The Incident Lead must escalate High Risk and Medium Risk Data Breaches to the response team (whose details are set out at the end of this protocol).
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the response team.

Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

1. The response team is to take any further steps (i.e., those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.
2. The response team is to work to evaluate the risks associated with the Data Breach, including by:
    a. Identifying the type of personal information involved in the Data Breach.
    b. Identifying the date, time, duration, and location of the Data Breach.
    c. Establishing who could have access to the personal information.
    d. Establishing the number of individuals affected; and
    e. Establishing who the affected, or possibly affected, individuals are.
3. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach; in which case it should be treated as an EDB.

The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise and EDB.

All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

Phase 3. Consider Data Breach Notification

1. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.
2. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been and EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.
3. After completing the statement, unless it is not practicable, the response team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are risk from the EDB.
4. If it is not practicable to notify some or all of these individuals, the response team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to individuals.

Phase 4. Take action to prevent future Data Breaches

1. The response team 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.
2. The Compliance Lead or delegate must enter details of the Data Breach and response taken into a Data Breach log (CompliSpace). The Incident Lead or delegate must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
3. The Incident Lead or delegate must conduct a post-breach review to assess the effectiveness of the school's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.
4. The Incident Lead or delegate must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Protocol.
5. The Incident Lead or delegate must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

Response Team

The Data Breach Response Team consists of the following school staff. These staff co-ordinate other staff and third-party services required to respond to a data breach, based on their areas of responsibility:

Incident Leader	Deputy Principal
Incident Deputy	Director of Information Services
Compliance Manager	Executive Assistant
Staff	Head of School
Legal and Insurance	Business Manager
IT	IT Network Manager
Communications	Director of Development

* See contact details on page 12

Useful References

- 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 *
- ISCA and NCEC Privacy Compliance Manual, January 2018

Approved By: Executive Leadership Team
Contact Staff Member: DIS
Implementation Date: Nov 2021
Revision Date: Term 4 2022

Data Breach Workflow

Below is a workflow diagram provided by the OAIC to assist in the execution of the School's Data Breach response plan.