Data Breach Response Plan

Adopted: June 2023 Last Amended: Next Review: June 2025

Introduction

The plan sets out the procedure to manage a School's response to the actual or suspected unauthorised access to or disclosure or loss of personal information (**Data Breach**). Further guidance about responding to a Data Breach and an eligible data breach (**EDB**) under the notifiable data breaches scheme (**NDB Scheme**) is contained in Section 26.

Response plan

In the event of a Data Breach, School personnel 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 and Insurance advice should also be sought if necessary.

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

The School personnel who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the Business Manager or Principal. That person must take any immediately available steps 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.

In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.

The Principal or Business Manager must make a preliminary assessment of the risk level of the Data Breach. The following table sets out example 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.

Where a **High Risk** incident is identified, Principal or Business Manager must consider if any of the affected individuals should be notified immediately where serious harm is likely.

Principal or Business Manager must escalate **High Risk** and **Medium Risk** Data Breaches to the response team (whose details are set out at the end of this protocol).

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.

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.

The response team is to work to evaluate the risks associated with the Data Breach, including by:

1. identifying the type of personal information involved in the Data Breach;
2. identifying the date, time, duration, and location of the Data Breach;
3. establishing who could have access to the personal information;
4. establishing the number of individuals affected; and
5. establishing who the affected, or possible affected, individuals are.

The response team must then assess whether the Data Breach is likely to cause serious harm to any individual who 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 notifications.

The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it not strictly an EDB.

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 an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.

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 at risk from the EDB.

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 those individuals.

Phase 4. Take action to prevent future Data Breaches.

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 Principal or Business Manager must enter details of the Data Breach and response taken into a Data Breach log. The Business Manager must, every year, review the Data Breach log to identify any reoccurring Data Breaches.

The Principal or Business Manager 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.

The Business Manager must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.

If appropriate, a prevention plan is to be developed 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 Principal, Business Manager and Secretary form the response team.

Roles, responsibilities and authorities will be clearly articulated. Contact details will be available.

DATA BREACH RISK ASSESSMENT FACTORS

Consider who the personal information is about	
Who is affected by the breach?	Are pupils, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a pupil'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 (eg health records) or permanent information (eg 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 pupils who attend the School may not give rise to significant risk. However, the same information about pupils who have attended the School counsellor or students with disabilities, may be more likely to cause harm. The disclosure of names and address of pupils 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 pupil's name, address and grades without malicious intent (eg if the information is accidentally emailed to the teacher), the risk of serious harm to the pupil 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 (eg 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 pupils' domestic circumstances may be used to bully or marginalise the pupil 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 of 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 (eg younger students, students with disabilities/special needs, vulnerable families/parents)
What kind of kinds of information is involved?	Some information, such as sensitive information (eg health records) or permanent information (eg 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 may arise due to the context of the information involved. For example, a list of the names of some pupils who attend the School may not be sensitive information. However, the same information about pupils who have attended the School counsellor or students with disabilities
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 pupil 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 attacked 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 that 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 pupil's information without malicious intent, the risk of serious harm nay be unlikely.

What is the nature of the harm that could result from the breach?	Examples include identity thief, 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 pupils' domestic circumstances may be used to bully or marginalise the pupil 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 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 included loss if public trust in the School, damage to reputation, loss of assets (eg stolen laptops), financial exposure (eg bank account details are compromised), regulatory penalties (eg for breaches for the Privacy Act), extortion, legal liability, and breach of secrecy provisions in application legislation.