PENLEIGH AND ESSENDON GRAMMAR SCHOOL

If you require access to this policy in a language other than English, please contact the Principal's office on 9016 2000

Data Breach Response Plan

Rationale

Penleigh and Essendon Grammar School (the school) acknowledges its responsibilities to provide for efficient, confidential and safe utilisation of information and communication technology and management of data generated and/or stored by the school. We acknowledge the potential for harm that may result should a data breach occur. This document delineates the school's policy for proactive management and protection of data and sets out procedures and clear lines of authority in the event that the school experiences a data breach, or suspects that a data breach has occurred. The response plan observes the school's Privacy Policy and associated policies noted below.

Scope

This response plan applies to all members of the school community, including staff, students, parents and other external stakeholders including but not limited to also contractors, volunteers and Casual Relief Teachers.

Definitions

Data Breach

A data breach is any event that has caused or has the potential to cause unauthorised access to personal information held by the school in any format. A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of the school's ICT policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation from the data 'owner';
- viruses or other security attacks on IT equipment systems or networks;

- breaches of physical security, e.g. forcing of doors or windows into a secure room or filing cabinet containing confidential information;
- confidential information left unlocked in accessible areas, except when accessibility of this information is required for response to medical emergencies;
- insecure disposal of confidential paper waste;
- leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information;
- publication of confidential data on the Internet and social media sites;
- disclosure of passwords (whether deliberate or accidental);
- inadequate de-commissioning of office furniture (e.g. filing cabinets);
- misdirected emails or faxes containing identifiable personal, confidential or sensitive data.

Harm

Harm refers to the potential or actual impacts of a data breach on individuals, whether it is harm to their physical or mental wellbeing, financial loss, or damage to their reputation. Harm also refers to the potential or actual impacts of a data breach on the school's reputation and/or information assets.

Examples of harm include:

- Emotional and psychological harm
- Threats to an individual's physical safety
- Damage to reputation or relationships (individual and/or school)
- Loss of business or employment opportunities
- Identity theft
- Financial loss (individual and/or school).

Serious harm can relate to any of the examples listed above (physical, psychological, emotional, financial and reputation) where the impacts are deemed to be significant and/or severe. The definition of serious harm is not prescribed and will be applied as a decision of the Principal or Board of Directors.

Notifiable Data Breach Scheme

The Notifiable Data Breach Scheme (NDBS) commenced in February 2018 following the enactment of the *Privacy Amendment (Notifiable Data Breaches) Act 2017.* The NDBS scheme requires entities covered by the Act to notify not only individuals affected by the breach but also the Australian Information Commissioner (OAIC) when and where a data breach is likely to result in serious harm to the individuals affected. The Principal or Board of Directors will decide where serious harm is likely to result from an incident with associated notification requiremments.

Personal Information

Personal information is information about an identified individual, or an individual who is 'reasonably identifiable'. Information that is not about an individual on its own can become personal information when it is combined with other information and this combination results in an individual becoming 'reasonably identifiable'.

Preventative Practices

Staff and students are required to adopt practices to manage data effectively and which reduce the possibility of data breach. Users of the technology should:

- Take positive actions to avoid loss of portable devices or equipment containing identifiable personal, confidential or sensitive data;
- Avoid unauthorised use of information;
- Comply with the School's ICT policies;
- Ensure that confidential information is not left unlocked in accessible areas;
- Log-out of a user account before leaving IT equipment unattended and lock the screen to stop others accessing information;
- Do not publish confidential data on the Internet and social media sites;
- Do not disclose passwords to others;
- Take care to avoid misdirecting emails which contain identifiable personal, confidential or sensitive data;
- Always share documents in secure ways as described in the ICT Policy;
- Print confidential or private documents in a secure area where possible;
- Do not leave confidential or private documents in a non-secure area;
- Participate in training as offered to staff and students and apply recommendations.

In general and at all times, staff and students are urged to exercise due care and diligence in relation to these matters and to comply with the ICT Policy and Electronic Devices and Communication Policy for Students.

Procedures in Response to a Breach

Data Breach Incident Alerts

Where a data breach is known to have occurred (or is suspected) by any member of the school community, or by its contractors and service providers, the person(s) who becomes aware of this must in the first instance alert the Privacy Officer and, if relevant, the Director of ICT.

The alert should include when the breach occurred or was first suspected (time and date); a description of the breach or suspected breach; the type of personal information involved; cause of the breach (if known); how it was discovered; which system(s) if any are affected (if known); and whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

Data Breach Response Team

The school's Data Breach Response Team is responsible for carrying out the actions that reduce the potential impact of a data breach and that achieve a resolution to the cause and impacts of the breach. The Data Breach Response Team includes the following staff:

- The Principal (Chair)
- The Director of ICT
- The Director of Finance
- The Privacy Officer

Depending on the nature and extent of the breach, other staff and external consultants may be consulted, such as a media/communications advisor, lawyer, cybersecurity expert or ICT forensics consultant.

Response Method

There is no single method of responding to a data breach. The data breach must be responded to on a case-by-case basis by assessing the rikss involved. The Team will be guided by a foure-step response process. These steps are:

1. **Containing the breach:** Take immediate steps to limit any further access to/disclosure of/loss of personal information
2. **Assessing the breach:** Gather the facts and evaluate the risks, including potential harm to affected individuals and, where possible, take action to remediate any risk of harm.
3. **Notifying affected individuals and relevant authorities if required:** If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify to OAIC. Consider others who should be notified, such as police or other organisations affected by the breach.
4. **Preventing future breaches:** Review the incident and take action to prevent further breaches, such as fully investigating the cause of the breach, developing a prevention plan, updating response plan and relevant policies and procedures, and if necessary, revising training practices for staff, and others able to access data including contractors, CRTs and volunteers.

Related Policies
Privacy Policy
Whistleblower Policy

Published: May 2023
To be reviewed: May 2025