# Data Breach Response Plan

**Rationale**

This Data Breach Response Plan (response plan) sets out procedures and clear lines of authority for staff in the event that the College experiences a data breach (or suspects that a data breach has occurred). The Data Breach Response Plan observes the Privacy Policy and associated referenced documentation.

This response plan is intended to enable the College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the College to respond to a data breach, including a notifiable data breach.

**Scope**

This response plan applies to all employees and other persons involved in the business and educational operations of Parade College.

**Data Breaches**

Under APP 11 (security of information), organisations are required to take reasonable measures to protect information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. The Notifiable Data Breach Scheme will require organisations to notify the Office of the Australian Information Commissioner (OAIC) and the affected individual(s), in the event of a notifiable data breach.

A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference as per 6.1 of the Parade College Privacy Policy.

Pursuant to section 26WE of the Privacy Amendment (Notifiable Data Breaches) Act 2017, an eligible data breach, which would require notification, occurs in circumstances where:

- There is an unauthorised access or unauthorised disclosure of information and a reasonable person would conclude that access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
- Information is lost in circumstances where such unauthorised access or disclosure is likely to occur and a reasonable person would conclude that, assuming such access or disclosure did occur, it would be likely to result in serious harm to any individuals to whom that information relates.

Where such breach occurs, the College undertakes to prepare a statement in accordance with the Privacy Amendment (Notifiable Data Breaches) Act 2017 and notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable after the school becomes aware of the eligible data breach except where exempted under the Act.

Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

**Internal reporting of a breach**

If a College staff member suspects a data breach has occurred they should immediately report the suspected breach to their line manager. The line manager will send a brief email to the College Privacy Officer that contains the following information:

- description of the breach or suspected breach
- immediate action taken by the line manager to address the breach or suspected breach (if any)
- the outcome of that action.

**Determining the seriousness of a data breach**

The College Privacy Officer will consider the following:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in the College's processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

Personnel from the following departments may be seconded to assist with the effect of the data breach:

- Principal
- Information Technology
- Marketing and Communications
- EREA VSL (Privacy Officer and/or Legal Advisory).

The College Privacy Officer will record all breaches on the College's Log of Breaches.

**Process**

1. The College experiences data breach/data breach suspected
    - Discovered by staff member or otherwise reported
2. What should the staff member do?
    - Immediately notify your line manager of the suspected breach
3. What should the line manager do?
    - Report the breach to the College Privacy Officer
4. What will the College Privacy Officer do?
    - Determine whether a data breach has or may have occurred
    - Determine the seriousness of the breach
5. If a breach has occurred, the College Privacy Officer will:
    - Arrange to contain the breach and make a preliminary assessment
    - Evaluate the risks for individuals of the breach
    - Review the incident and instigate action to prevent future breaches

- Consider whether the breach is notifiable and if so, complete notification.

**Steps for the College Privacy Officer**

**Step 1 - Contain the breach and make a preliminary assessment**

- Contain breach using seconded resources if necessary
- Provide ongoing updates to the Principal
- Ensure all evidence is preserved that may be valuable in determining the cause of the breach to allow swift and appropriate corrective action
- Alert Principal's Office in relation to media interest

**Step 2 - Evaluate the risks for individuals associated with the breach**

- Conduct initial investigation, and collect information about the breach promptly, including:
  - the date, time, duration, and location of the breach
  - the type of personal information involved in the breach
  - how the breach was discovered and by whom
  - the cause and extent of the breach
  - a list of the affected individuals, or possible affected individuals
  - the risk of serious harm to the affected individuals
  - the risk of other harms.
- Determine whether the context of the information is important.
- Establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.
- Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.

**Step 3 - Consider breach notification**

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
- Determine whether to notify affected individuals – is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals.
- Consider whether others should be notified, including EREA VSL, police/law enforcement, or other agencies or organisations affected by the breach.

**Step 4 - Review the incident and take action to prevent future breaches**

- Fully investigate the cause of the breach.
- Report to the Principal on outcomes and recommendations:
  - Update security if necessary
  - Make appropriate changes to policies and procedures if necessary
  - Revise staff training practices if necessary.