Updated: 2023

St Patrick's Data Breach Response Plan

This data breach response plan (response plan) sets out procedures in the event that St Patrick's experiences a data breach (or suspects that a data breach has occurred).

Definition
Data Breach - A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. 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.

Notifiable Data Breach - Where a data breach has occurred that is likely to result in serious harm to any of the individual to whom the information relates, it is considered 'eligible' and must be reported to the Office of the Australian Information Commissioner (OAIC)

Implementation
This response plan is intended to enable the St Patrick's to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It clarifies the roles and responsibilities of staff, and the processes to assist the school to respond to a data breach (refer to Appendix A: Flow Chart: Data Breach Response Plan).

Some data breaches may be comparatively minor, and able to be dealt with easily without reporting to the OAIC. For example:

> A staff member, as a result of human error, sends an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that the issue is reported to the principal but does not require any further response.

This should be documented including:

- Description of breach or suspected breach
- Action taken by the principal to address the breach or suspected breach
- The outcome of the action
- The principal's view that no further action is required

The principal will use their discretion in determining whether a data breach or suspected data breach requires an escalation of the data breach process. In making that determination, principal will consider the following questions:

- 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 school processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the principal to notify the OAIC (refer to Risk Assessment Process).

OAIC Advice Data Breach: What must be included will assist the principal in notifying the OAIC.
https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guideaugust-2014.pdf

Record Management

Documents on breaches will be saved in a central file on school administration system.

Refer to:

- Appendix A: Flow Chart: Data Breach Response Plan
- Appendix B: Risk Assessment Process
- Appendix C: Data Breach Prevention Checklist (CECV)
- Appendix D: Individual Notification Record (CECV)
- Appendix E: Example of an Email to Parents/Carers (CECV)
- Appendix F: Data Breach Notification for Other Entities (CECV)
- Appendix G: Notification Procedures Checklist (CECV)
- Appendix H: Contain the Breach and Preliminary Assessment (CECV)
- Appendix I: Evaluate Risks (CECV)