ST JOSEPH'S COLLEGE, MILDURA

Policy Number:	COLLEGE 33
Policy Name:	Data Breach Response Policy
Contact Officer:	Business Manager
Date Approved by Executive:	April 23, 2019
Date of Next Review:	April 2022
Related Policies:	Standard Collection Notice Privacy Policy Data Breach Response Plan

PREAMBLE

God is at the centre of our College…Mercy is the heartbeat of the Gospel. We encourage every student to grow in the fullness of life and realise their potential through the bread we break at school, the bread of relationships and the bread of conversation. Let us engage the heart and bring faith to life and life to faith (Thomas Groome).

LEGISLATION

This policy takes into account relevant legislative requirements within the state of Victoria, including the specific requirements of the Victorian Child Safe Standards as set out in *Ministerial Order No. 870.* This policy applies to St Joseph's College staff, including employees, volunteers, contractors and clergy.

1. WHAT IS A PERSONAL INFORMATION DATA BREACH AND HOW DOES IT OCCUR?

1.1 A Personal Information Data Breach occurs when official information that is not already publicly available, is lost or subjected to unauthorised access, use modification, disclosure or misuse. Personal Information Data Breaches may occur in a number of ways, including accidental loss, internal errors or deliberate actions of trusted employees, theft of physical assets or the theft or misuse of electronic information (e.g. a cyber-attack).

1.2 Data breaches of personal information are regulated by the Privacy Amendment (Notifiable Data Breaches) Act 2017.

2. WHAT IS PERSONAL INFORMATION?

2.1 Personal information is information or an opinion, whether true or not, relating to a natural person, or the affairs of a natural person, whose identity is apparent, or can reasonably be ascertained. A natural person is in this context is a living human being. Personal information can include combinations of name, address, date of birth, financial or health details, ethnicity, gender, religion, etc. The personal information held by an agency may be collected in paper form, verbally or through electronic means.

3. WHAT IS UNAUTHORISED ACCESS?

3.1 Unauthorised access of personal information occurs when personal information is accessed by somebody who is not permitted to have access to it. This could include a student, student's family, employee or contractor to whom we have not given permission to access.

4. WHAT IS UNAUTHORISED DISCLOSURE?

4.1 Unauthorised disclosure of personal information occurs when confidential information is disclosed to outside parties in a way that is not permitted under the Privacy Act.

5. WHAT IS LOSS OF INFORMATION?

5.1 Loss of personal information refers to the accidental or inadvertent loss of personal information held by us in circumstances, which are likely to result in unauthorised access or disclosure. For instance, if one of our employees leaves personal information on public transport.

6. TO WHOM DO WE REPORT DATA BREACHES?

6.1 Staff, volunteers, parents and students are required to inform the College of a data breach or any suspicions of a data breach.

6.2 Please inform the:

- Personal Assistant to Principal – taston@sjcmda.vic.edu.au
- Risk, Compliance and Asset Manager - whenderson@sjcmda.vic.edu.au

6.3 In the absence of the Personal Assistant to Principal, please inform a member of the College Executive.

6.4 Once informed the person(s) will then follow the Data Breach Response Plan for further action.

7. HOW DO WE ASSESS THE SERIOUSNESS OF A DATA BREACH?

7.1 In assessing whether the data breach is likely to result in serious harm, we may consider some of the following information:

- The kind or kinds of information breached;
- The sensitivity of the information breached;
- Whether the information is protected by one or more security measures;
- The persons or kinds of persons who have obtained, or who could obtain the information;
- If security technology or methodology was used, and whether the technology or methodology was designed to make the information unintelligible or meaningless to persons who are not authorised to access the information;
- The nature of the harm; and
- Any other relevant matters.

Refer to the Data Breach Response Plan – Risk Assessment Process and Risk Assessment Checklist.

8. HOW DO WE RESPOND TO A DATA BREACH?

8.1 Follow and refer to the Data Breach Response Plan.

8.2 The Principal or member of College Executive in conjunction with the Risk, Compliance & Asset Manager (RCAM) will conduct an initial risk assessment to determine the seriousness of the breach or suspected breach.

8.3 The Principal or member of College Executive, or if directed the RCAM, will inform Mercy Education Ltd of the breach if the initial assessments determine the breach to be of serious nature.

8.4 The RCAM will inform the Data Breach Response Team (As per Data Breach Response Plan), and will coordinate the reviews, audits, investigations and any documentation recording and saving.

8.5 The Data Breach Response Team will follow the Data Breach Response Plan (DBRP). Each member must document and use the checklist or templates provided in the plan. These include:

- Flow Chart (DBRP – Appendix A)
- Data Breach Prevention Checklist (DBRP – Appendix B)

- Breach Containment & Preliminary Assessment Checklist (DBRP – Appendix C)
- Risk Assessment Procedure & Assessment Checklist (DBRP – Appendix D)

9. DATA BREACH ASSESSMENT & NOTIFICATION PROCESS

9.1 Once it is ascertained that a Personal Data Breach is likely to have occurred, the College will assess the risks associated with the data breach and whether affected parties should be notified. Please follow the Data Breach Response Plan.

9.2 If a data breach creates a real risk of serious harm to an individual or organisation, the affected parties should be notified. However, it will not always be appropriate. Providing notification about low risk breaches can cause undue anxiety and de-sensitise individuals to notice. Please refer to the Data Breach Response Plan.

9.3 Each incident needs to be assessed on a case-by-case basis to determine whether notification is required. Prompt notification to those affected in these cases can help them mitigate the damage by taking steps to protect themselves. The College must ensure that complete records are maintained of each incident with all Checklist completed and notification records as per the Data Breach Response Plan (DBRP).

9.4 Notifying affected parties – As per the Data Breach Response Plan, must complete the Notification Records:

- Individual Notification Record (DBRP – Appendix E)
- Organisational Notification Record (DBRP – Appendix F)

9.5 At the point that notification is being considered, the College should have as many facts as possible and have completed a risk assessment. Sometimes the urgency or seriousness of the incident dictates that notification should happen immediately, before having all the relevant facts.

10. IMPORTANT CONSIDERATIONS

10.1 Notifying parties affected by a data breach is considered good practice. It can promote open and transparent dialogue and assist in rebuilding trust.

10.2 The decision on how to notify should be made on a case-by-case basis. In some cases, the College may choose to take additional actions that are specific to the nature of the incident.

10.3 As part of the initial assessment of a security incident, the company's CEO should be immediately informed. Law enforcement, internal investigation units, across government response organisations and other regulatory bodies should also be notified as required by relevant policy or legislation.

10.4 Where law enforcement authorities are investigating the incident, consult the investigating agency before making details of the incident public.

11. CONTACT ORGANISATIONS FOR ADVICE

11.1 In addition to notifying those affected by a data breach, data breach response plans should include a list of other parties that may need to be notified. Below is a list of organisations that the manager responsible may be required to notify, or may consider notifying, if a data breach occurs.

Police

- If the data breach is a result of criminal actions the Police should be notified as soon as practicable.
- Delay the notification of those affected by the data breach until advice from the Police is given, as notification may compromise a criminal investigation.
- The Police can be contacted by telephone, or visit your local Police station.

Office of the Australian Information Commissioner

- If the data breach relates to tax file number (information), and it is likely that it will result in serious harm to individuals, the Office of the Australian Information Commissioner (OAIC) must be advised in accordance with the Australian Government's Notifiable Data Breaches Scheme (The Scheme).
- The Scheme specifies the information that must be included in the notifications for those affected, the timeframe for notification i.e. as soon as practicable within 30 days of the breach being discovered, and the requirement to notify the Australian Information Commissioner of the breach.
- Contact details and information on how to report a breach to the OAIC can be found at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme. Please also refer to the Data Breach Response Plan.

12. ADDITIONAL CONTACTS

12.1 You may also need to contact:

- **Any other organisation that is the source of the information that was compromised**: For example, if Tax File Numbers or Medicare Numbers were contained the information that was compromised, the Australian Taxation Office or Medicare respectively should also be notified of the breach.
- **Insurers (CCI):** If required by contractual obligations or to access Cyber Risk Insurance.
- **Financial institutions or credit card companies:** This may be to assist you in notifying individuals or reducing the impact on those affected.
- **Other internal or external parties:** Consider if any other third parties may have been affected by the breach. For example, if information about a particular government tender process was breached, all organisations that submitted a tender, even if their information wasn't included in the breach, may need to be notified. Some parties to consider include:
    - Other internal business units not already notified that may have a need to know (e.g. communications, human resources, senior management group);
    - Government departments that may experience some impact from the breach. Unions or other employee representatives, particularly if any employee information was compromised.

13. REGULATORY BODIES

- Australian Securities and Investment Commission: Companies and registered corporations may have reporting requirements to ASIC.
- Australian Competition and Consumer Commission (ACCC): The ACCC has a role in protecting the interests and safety of consumers and as such they have their own data breach notification requirements. Also consider if individuals affected may contact the ACCC to make a complaint regarding the data breach.
- Australian Communications and Media Authority (ACMA): ACMA have their own data breach reporting requirements if the data compromised includes Integrated Public Number Database (IPND) information.
- Other regulatory bodies: The Education, Infrastructure, Health, Justice and Child Protection Sectors in particular may have specific regulatory bodies that require notification in the case of a data breach.