# Star of the Sea College

# Data Breach Response Plan

**OBJECTIVE OF THE DATA BREACH RESPONSE PLAN (Plan)**

The Privacy Act 1988 (**Privacy Act**) requires all government agencies, organisations, schools and Catholic colleges, including Star of the Sea College (**College**) to put in place reasonable security safeguards and to take reasonable steps to protect the personal information that they hold from misuse, interference and loss and from unauthorised access, modification or disclosure.

The objective of this Plan is to ensure that the College takes reasonable steps (including implementing this Plan) to meet its obligations under the Privacy Act to safeguard personal information and act in the best interests of its students and College staff.

The 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 staff and/or students
- provide contact details for the appropriate staff member 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
- assist the College to meet its obligations under the Australian Government's Notifiable Data Breach (**NDB**) scheme,
- ensure that affected individuals are notified about serious data breaches as well as the Australian Information Commissioner.

The Australian Government developed the NDB scheme to apply to all businesses, government agencies and schools, including the College covered by the Privacy Act. The scheme is to be administered by the Office of the Australian Information Commissioner (**OAIC**) under the Privacy Amendment (Notifiable Data Breaches) Act 2017 and will commence on 22 February 2018. Data breaches that occurred before this date will not be covered under this NBD scheme.

**PLAN SCOPE**

This Plan is to be read in conjunction with the Star of the Sea College's (**College**) Privacy Policy.

This Plan applies to all employees, including external service providers, contractors (independent and volunteers), Board and Committee members of the College.

## DEFINITIONS

### Data Breach

A data breach is when personal information held by the College is **lost** or subjected to **unauthorised access**, modification, **disclosure**, or other misuse or interference. Examples of a data breach are when a device containing personal information of a student is lost or stolen, the College's database containing personal information is hacked or the College mistakenly provides personal information to the wrong person. Data breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failure to follow information handling policies that cause accidental loss or disclosure.

**Loss** refers to the accidental or inadvertent loss of personal information held by the College, in circumstances where is it is likely to result in unauthorised access or disclosure. An example is where a student leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.

**Unauthorised access** of personal information occurs when personal information that the College holds is accessed by someone who is not permitted to have access. This includes unauthorised access by a teacher, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

**Unauthorised disclosure** occurs when the College makes personal information accessible or visible to others outside the College, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by external service provider of the College.

Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach. For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

**Notifiable (Eligible) Data Breach** - A Notifiable (or eligible) Data Breach (**NDB**) is a data breach that is likely to result in **serious harm** to any of the teachers, students, College employees or individuals to whom the information relates. A notifiable or eligible data breach arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the College holds; (see above definition of **Data Breach**)
- this is likely to result in serious harm to one or more individuals; (see below) and
- the College has not been able to prevent the likely risk of serious harm with remedial action.

**Serious Harm**

The second step in deciding whether a notifiable data breach has occurred involves deciding whether, from the perspective of a reasonable person, **the data breach would be likely to result in serious harm to an individual** whose personal information was part of the data breach.

For the NDB scheme a '**reasonable person**' means a person in the College's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach.

The phrase '**likely to occur**' means the risk of serious harm to an individual is more probable than not (rather than possible). The chance that an individual will experience serious harm increases as the number of people whose personal information was part of the data breach increases.

**'Serious harm' is not defined in the Privacy Act.** In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, economic, financial, or reputational harm.

In assessing the risk of serious harm, the College should consider the broad range of potential kinds of harms that may follow a data breach. For example:

- identity theft
- significant financial loss by the College
- threats to an individual's physical safety
- humiliation, damage to reputation or relationships and
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

**OAIC** - Office of the Australian Information Commissioner

**Personal Information** - Personal information is information or an opinion about an identified, or reasonably identifiable, individual. It may include contact and student identification information: scholarship or special fee information, name, address, telephone number, email address and date of birth; and other identification verification information, including photographic information, from documents including birth certificate, student card, passport, driver's license, citizenship certificate, tax notice assessments and utilities notices

## DATA BREACH RESPONSE – KEY PROCESSES

- Implementation – developing and implementing a data breach response plan may assist in protecting the College's assets – personal information and mitigating costs – financial and reputational associated with a breach of personal information.

- Timeliness – a quick response to a data breach can substantially decrease the impact students, teachers and other College staff and address the potential disruption caused by a breach of personal information.

- Compliance – a data breach response plan can assist the College to meet its Privacy Act obligations, support general risk management and compliance procedures (including breach and incident reporting) and enhance insurance protections across all business units.

- Communications strategy – an effective data breach response plan provides for liaison with external stakeholders, insurers, appropriate 'media' management and immediate notification (communication) with affected individuals (clients) and appropriate government agencies as required by the Privacy Act (and the NDB scheme) – OAIC and ASIC.

## OPERATIONAL DATA BREACH RESPONSE PROCEDURES

This operational data breach response plan establishes the steps and clear lines of authority for the College staff if the College experiences a data breach (or suspects that a data breach has occurred).

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 and organisations.

**The College Experiences Data Breach / Data Breach Suspected**

eg, discovered by a College Teacher

↓

**What Should the College Teacher Do?**

- Immediately notify the Risk & Compliance Manager of the suspected data breach

↓

**What Should the Risk & Compliance Manager Do?**

- Determine whether a data breach has or may have occurred.
- Determine whether the data breach is serious enough to escalate to the Data Breach Response Team (some breaches may be able to be dealt with by IT).

↓

**Notify the College Data Breach Response Team**

The Principal, the Chairman of the Governance & Risk Committee, the Business Manager and the IT Manager

**DATA BREACH ANALYSIS**

The Risk & Compliance Manager will make an initial assessment of the data breach and decide (exercise discretion) whether to notify the Principal and the College's Data Breach Response Team (**DBRT**). The Risk & Compliance Manager will consider the data breach assessment criteria before referring an issue to the DBRT, including but not limited to:

- Number of students, teachers and the College's staff affected;
- Risk of harm (serious harm) – level of harm $ impact;
- Breach of contract –clauses in third party agreements to keep information secure and confidential;
- Evidence of compliance failure or systemic problems; and
- Possible media, College reputational impact.

Minor data breaches may be handled / resolved at the operational level and recorded in the College's incident register.

Serious data breaches must be advised to the DBRT:

- IT Manager;
- Business Manager;
- The Principal and
- The Chairman of the Governance & Risk Committee

The DBRT to advise the Leadership Team and develop response to data breach – possible steps (also refer to Checklist – see Appendix). The DBRT should ideally undertake steps 1,2 and 3 either simultaneously or in quick succession.

**Step 1 – contain breach and make a preliminary assessment**

- Convene a meeting of the DBRT
- Immediately contain breach:
  - IT to implement the IT Disaster Recovery Plan if necessary
  - Building security to be alerted if necessary
- Inform the OIAC within the required timeframe
- Ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing the OAIC to take appropriate corrective action
- Consider developing a communications or media strategy to manage public expectations and media interest

**Step 2 – Evaluate the Risks Associated with the Breach**

- Conduct initial investigation – gather 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 cause and extent of 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.

The College should conduct this assessment expeditiously and, where possible within 30 days, If it cannot be done within 30 days, document why this is the case.

**Step 3 –Breach Notification**

- Determine who needs to be made of aware of this 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 individual? In some cases, it may be appropriate to notify the affected individuals immediately; eg where there is a high level of risk of serious harm to affected individuals.
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisation/s affected by the breach.

**Step 4 – Prevent Future Breaches**

- Full investigation of cause of breach
- Report to the Principal, the Leadership Team, the Governance & Risk Committee and the Board and make recommendation:
  - Update security and response plan if necessary
  - Make appropriate changes to policies and procedures if necessary
  - Revise staff training practices if necessary
  - Consider the option of an audit to ensure necessary outcomes are affected

Data breaches and remediation to be reported via the College's Incident Register and considered by the Governance & Risk Committee and reported to the Board.

**REVIEW**

This data breach response plan will be reviewed and updated on a regular basis and at least every 2 years

**APPENDIX -Data Breach Response Plan Quick Checklist**

Use this list to check whether your response plan addresses relevant issues.

| Issue | Yes/No | Comments |
|---|---|---|
| How is data breach identified? | | |
| Do your staff know what to do if they suspect a data breach has occurred? | | |
| Who is on your response team? | | |
| Has the Risk & Compliance Manager, the IT Manager and Business Manager been notified? | | |
| Do you need to include external expertise in your response team, ie data forensics experts, privacy expert? | | |
| Has details of breach recorded? | | |
| Has the context of breach established | | |
| Is this a minor or serious breach? | | |
| When do you notify individuals affected by a data breach? | | |
| Principal / Leadership Team informed? | | |
| Notification to insurers, clients, external stakeholders, regulators and/or law enforcement? *Notifiable Data Breach* scheme – students/teachers and OAIC | | |
| Do you have an agreed approach on communication strategy – staff, clients, media management? | | |
| Is Cause of breach established and remedial action implemented? | | |
| Breach reported in the *Issues Register* | | |
| Follow-up plan review, procedure updates, training, audit and testing | | |

| | |
|---|---|
| **Responsible Officer** | The Principal |
| **Approved By** | Risk & Compliance Manager |
| **Approved and Commenced** | 22 February 2018 |
| **Review By** | IT Manager, the Business Manager, the Leadership Team |
| **Relevant Legislation** | Part IIIIC of the Privacy Act (Cth) 1988<br>Privacy Amendment (Notifiable Data Breaches) Act 2017 |
| **Related Policies & Procedures** | IT Disaster Recovery Plan<br>Critical Incident Management Policy and Procedures<br>Business Continuity Plan |
| **Version** | 1 |
| **Amendments to Version** | |