Review Date:	**August 2019**
Authorised by:	**Principal**
Contacts:	**Business Manager/Head of IT**
Locations:	**SS2/MyS/SW**

DATA BREACH POLICY

1. RATIONALE

A key risk for organisations in the digital age is a lack of customer trust and confidence in an organisation's data storage and sharing arrangements. As more and more information is being held in electronic format, the risk of breaches in security protecting that data has also greatly increased.

2. SCOPE

This policy applies to Notifiable Data Breaches where personal information held by the School is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference **AND** is likely to result in serious harm to any of the individuals to whom the information relates. Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

This response plan is applicable to all members of the School community – students, parents, staff and related parties, such as creditors, donors, suppliers.

3. BACKGROUND

The Notifiable Data Breach amendment to the Privacy Act closes one of the gaps in the legislation, with the requirement for an organisation to report breaches rather than waiting for an injured party to notice that their data was being misused and then complaining about it.

4. POLICY STATEMENT

4.1 Schools are required to take 'reasonable steps' to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

The Federal Privacy Act makes it compulsory for schools to notify specific types of data breaches (Notifiable Data Breaches or NDBs), to:

4.1.1 individuals affected by the breach, and
4.1.2 Office of the Australian Information Commissioner (OAIC).

5. PROCEDURES

5.1 What is a Notifiable Data Breach?

Under the Act a data breach must be notified where:

- there is unauthorised access to, or unauthorised disclosure of, personal information; and
- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the personal information relates.

OR

Personal information is lost in circumstances where:

- unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
- assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

5.2 What Needs to Happen When there has been a Notifiable Data Breach?

Where an eligible data breach is suspected or believed to have occurred, Somerville House will:

- carry out a risk assessment in the event that an eligible data breach is suspected;
- prepare a statement of prescribed information regarding an eligible data breach that is believed to have occurred;
- submit the statement to the OAIC; and
- contact all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

5.2.1 Risk Assessment

If Somerville House suspects an eligible data breach may have occurred or received a complaint in relation to the security of personal information, it will conduct a risk assessment which involves:

- assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This must be as prompt and efficient as practicable in the circumstances; and
- taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

If the risk assessment reveals that an eligible data breach has occurred, Somerville House will then follow the notification requirements under the Act and notify both the OAIC and if practicable, the individual/s affected.

5.2.2 Notification of OAIC

Once Somerville House has reasonable grounds to believe that there has been an eligible data breach, it will:

- prepare a Statement in the prescribed format; and
- provide a copy of the Statement to the OAIC as soon as practicable after the School becomes aware of the eligible data breach.

The Statement will include:

- the identity and contact details of the School;
- a description of the eligible data breach that the School has reasonable grounds to believe has happened;
- the kind/s of information concerned; and
- recommendations about the steps that individuals should take in response to the eligible data breach that Somerville House has reasonable grounds to believe has happened.
- If Somerville House believes that another entity regulated by the Act is involved in the eligible data breach, the Statement must include information about the other entity/ies.

5.2.3 Notification of Individuals

- As soon as practicable after notifying the OAIC, Somerville House will:
- notify each of the individuals to whom the relevant information relates; or
- notify each of the individuals who are at risk from the eligible data breach.

In each case, Somerville House will take "such steps as are reasonable in the circumstances" to notify the individuals. What is practicable will involve considerations about the time, effort or cost of a notification and most likely in the circumstances to be effective in bringing the eligible data breach to the attention of affected individuals.

If Somerville House is unable to notify individuals, it will:

- publish a statement on its website; and
- take reasonable steps to publicise the contents of the Statement prepared for the OAIC.

5.2.4 Remedial Action

Where an unauthorised access or disclosure of personal information occurs but appropriate remedial action is taken, this may avoid triggering the eligible data breach notification procedures.

If remedial action is taken before the unauthorised access or disclosure causes serious harm to any of the individuals to whom the information relates, and as a result of that action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals, the access or disclosure will not be an eligible data breach.

5.2.5 Data Breach Response Plan

A data breach response plan is one tool to help Somerville House manage a data breach. It is a framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken in managing a breach if one occurs.

The Somerville House Data Breach Response Plan is included in Appendix 1 of this policy.

Having a data breach response plan is part of establishing robust and effective privacy procedures and having clear roles and responsibilities is part of good privacy governance.

Our data breach response plan helps Somerville House to:

- meet our obligations under the Privacy Act
- protect an important business asset
- deal with adverse media or stakeholder attention from a breach or suspected breach
- instill public confidence in our capacity to protect personal information by properly responding to the breach.

6. BREACH

If you breach this policy you may be subject to disciplinary actions.

7. REFERENCES

7.1 Other Related Policies

- Privacy Policy
- Computer Use Policy

7.2 Legislative and other References

- Privacy Act 1988 (Cth)

8. RESPONSIBILITIES

Council
- Ensure compliance with legislative requirements.

Principal
- Oversight of compliance with this policy.

Business Manager
- Convenes Data Breach Team

9. REPORTING REQUIREMENTS – Guidelines for Staff

9.1 Notify OAIC and affected parties

10. DEFINITIONS

Data Breach - occurs where "personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference."

Notifiable Data Breach - data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

Serious Harm could include serious physical, psychological, emotional, economic or financial harm, as well as serious harm to reputation.

11. ATTACHMENTS

1. *Data Response Plan*
2. *ISQ Notifiable Data Breach Definition*
3. *ISQ Serious Harm Definition*

Version Control Table			
Version Control	**Date Effective**	**Approved By**	**Amendment**
1	August 2019	Principal	

Appendix 1- Data Response Plan

SOMERVILLE HOUSE DATA BREACH RESPONSE PLAN

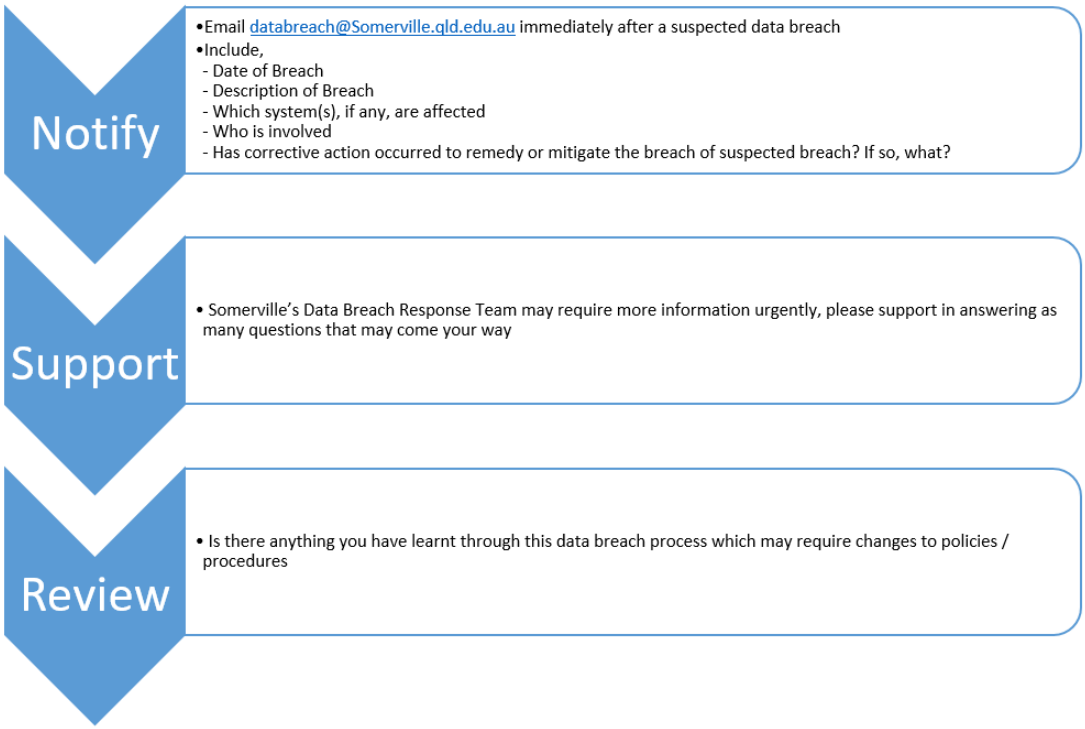
1. Somerville House Experiences Data Breach or a Data Breach is Suspected

Discovered by Somerville House staff member, or Somerville House otherwise alerted.

2. What Should A Somerville House Staff Member Do?

Immediately notify databreach@somerville.qld.edu.au of the suspected data breach.

(a) time and date the suspected breach was discovered;
(b) the type of personal information involved;
(c) the cause and extent of the breach (if known); and
(d) context of the affected information and the breach.



3. What should the Head of ICT 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 Incident Team.
- If so, immediately escalate to the Data Breach Incident Team.

4. Alert Business Manager

Business Manager to convene Data Breach Team meeting, consisting of:

- Principal
- Business Manager
- Director of Communications and Admissions
- Head of ICT

Notifiable data breach

1. Unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals (**the affected individuals**)

2. A reasonable person would conclude that it would be likely to result in serious harm to the affected individuals.

Serious harm

Whether a reasonable person in the school's position would conclude that the data breach would be likely (more probable than not) to result in serious harm to any of the individuals to whom the information relates.

Serious harm may include serious physical, psychological, emotional, financial or reputational harm

Appendix 3 –

Probability	Impact: Trivial	Minor	Moderate	Major	Extreme
Rare	Low	Low	Low	Medium	Medium
Unlikely	Low	Low	Medium	Medium	Medium
Moderate	Low	Medium	Medium	Medium	High
Likely	Medium	Medium	Medium	High	High
Very likely	Medium	Medium	High	High	High

Impact Criteria

Trivial	Isolated local negative perception	Affects small number of (<10)	Negligible regulatory and/or contractual. Breach not reportable
Minor	Sustained local negative perception	May involve 50 data subject – no sensitive data	Minor regulatory and/or contractual breach, reportable
Moderate	Sustained local and/or regional perception	May involve 100+ data subject or relates to sensitive data	Regulatory censure and/or contractual breach, reportable
Major	Sustained regional and/or national negative perception	May affect 500+ data subjects. Remediation is likely to be time consuming and complex	Regulatory fines and/or significant corporate breach
Extreme	Sustained negative national perception	Affects significant numbers of data subjects (>1000+). Remediation is likely to be time consuming and complex, tracked at a senior level and related to sensitive information	Corporate litigation

Probability Criteria

Rare	One off incident will not be repeated
Unlikely	May happen again, but remedial actions make this unlikely
Moderate	Could happen again but remedial action has reduced this likelihood
Likely	Is likely to happen again within 1-7 days unless action is taken
Very Likely	Is likely to happen again almost immediately unless action is taken ASAP