Data Breach Response

Quick Reference Guide

A privacy breach occurs which an individual's personal information is subject to loss, unauthorised access, modification, disclosure or other misuse or interference.

This may be as a result of a malicious breach of the secure storage or information handling protocols. For example a cyber-security incident, accidental loss of IT equipment or hard copy documents, negligence, improper disclosure of information, or otherwise.

References to **personal information** includes information or an opinion about an identified individual or an individual who is reasonably identifiable; whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not. Examples include an individual's name, address, contact number and email address.

Special obligations apply to the collection of personal information that is sensitive information. **Sensitive information** includes for example, information about a person's race, religion, political views, sexual preference, criminal convictions, membership or professional membership, trade associations/unions or health information.

Common examples of data breaches include:

- lost or stolen laptops, removable storage devices, or paper records containing personal and/or sensitive information;
- hard disk drives and other digital storage media (whether integrated or not, into other devices for example multifunction printers) being disposed of or returned to equipment lessors without the contents first being properly erased;
- databases containing personal information being hacked or otherwise illegally accessed by individuals outside the University;
- personnel accessing or disclosing personal information outside the requirements or authorisation of their position/employment;
- paper records containing personal information of students, patients or other persons inappropriately disposed of through insecure means;
- paper records stolen from insecure recycling or garbage bins;
- mistakenly providing personal information to the wrong person, for example by sending correspondence out to the wrong address; and
- an individual deceiving an organisation into improperly releasing the personal information of another person.

It is critical that any evidence and/or records about a breach/incident are maintained to help with the investigation, notification and reporting processes.

The University is an entity that is covered by Victorian Privacy legislation, however there are some instances where the University has obligations under the Privacy Act 1988 (Cth) for example:

- as an organisation that is a tax file number recipient;
- as a private health service provider; and
- some contractual arrangements including those with Commonwealth Government agencies.

Under the Commonwealth Privacy legislation the notifiable breaches scheme requires organisations to notify individuals and the Office of the Information Commissioner about 'eligible data breaches'. An **eligible data breach** arises when the following three criteria are satisfied:

i) There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
ii) It is likely to result in serious harm to one or more individuals; and
iii) The University has not been able to prevent the likely risk of serious harm with remedial action.

Serious harm is not defined in the Privacy Act but in the context of a data breach, **serious harm** to an individual may include serious physical, psychological, emotional, financial or reputational harm. Examples of scenarios that could result in serious harm and the likelihood of each occurring may include:

- Identity theft
- Significant financial loss by the individual
- Threats to an individual's physical safety
- Loss of business or employment opportunities
- Humiliation, damage to reputation or relationships
- Workplace or social bullying or marginalisation

Some kinds of personal information are more likely to cause an individual serious harm if compromised. Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- Sensitive information such as information about an individual's health
- Documents commonly used for identity fraud (including Medicare card, driver licence, passport details)
- Financial information
- A combination of personal information (rather than a single piece of personal information)

Data Breach Incident Response Plan

Data Breach Occurs

You know there has been an eligible data breach when the following happens:
(a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information (staff and/or student personal information);
(b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

Step 1:

If you know or suspect a breach:

- take step to contain the breach
- notify the Privacy Officer

Contain and Notify
Business area takes steps to immediately contain the breach and notify the Privacy Officer as soon as possible. It is also important to preserve any evidence and records as part of the investigation process.

Step 2:

Assess and remediate

Preliminary Assessment and Remediation
Once immediate containment has occurred, the business unit with support from the Privacy Officer and other areas as needed, will conduct a preliminary assessment of the breach to develop a Remediation Plan:
- what information was involved i.e the sensitivity of information;
- the extent of the breach;
- potential harm to individuals;
- steps to be taken to mitigate the potential harm

The cause of the breach may not be able to be discovered in this phase.

In evaluating the risks and consider:

- The type of personal information involved
  - What is the level of harm; who is affected?
- The context of the affected information and the breach
  - Who has gained unauthorised access; how could the information be used?
- Where possible, the cause of the breach
  - Risk of ongoing breaches; is the information adequately encrypted; what mitigation has been taken?
- The risk of serious harm to the affected individuals
  - Who is the recipient; what are the consequences?
- The risk of other harms
  - Loss of public trust; reputation; regulatory penalties

Step 3:

Formal report

Formal Reporting
The Privacy Officer will evaluate the breach and assess what formal reporting is required.

Where the access, disclosure or loss is likely to result in serious harm to an individual, the University must notify the affected individuals and may need to notify the State or Federal Privacy Commissioner/s.

The Privacy Officer will also consider whether other entities, such as police, law enforcement or regulatory bodies need to be notified

A breach will be reported to Corporate Governance, Audit and Risk Committee of Council

Step 4:

Review the incident and revise practices

Review and Prevention

Business area in consultation with the Privacy Officer:
- Fully investigate the cause of the breach.
- Prepare a Prevention Plan to reduce the possibility of a future breach and mitigate the potential harm which might include updating Business Continuity Plans, revising existing policies, procedures and staff training.

Data Breach Roles and Responsibilities

When a data breach has occurred or is suspected to have occurred

Staff member:

- Immediately notify their Manager and the Privacy Officer of the breach.
- Record and advise:
  - The time and date of discovery;
  - The type of personal information involved;
  - Cause and extent of the breach; and
  - The context of the affected information
- Preserve any evidence and/or records to help in the investigation, notification and reporting processes.

Manager:

- Take immediate steps to contain the breach.
- Notify the Privacy Officer to report the incident as soon as possible (within 24 hours of detecting the breach).
- Preserve any evidence and/or records to help in the investigation, notification and reporting processes.
- Liaise with the Privacy Officer and Risk Management as part of the investigation, action and reporting processes.
- Complete the Privacy Incident Report.

Privacy Officer:

- Make a determination whether a breach has occurred;
- Consider whether immediate action can reduce further loss or mitigate damage;
- Determine severity and whether breach needs to be escalated; and
- If breach is likely to result in serious harm, notify the Executive Director Planning & Governance and where necessary instigate the Critical Incident and Emergency Management Procedures.
- Undertake any notification and formal reporting under the direction of the Executive Director Planning & Governance.

Critical Incident and Emergency Management Response Team

- Investigate the severity of the breach and determine the likelihood of serious harm.

Data Breach Response Plan

Internal contact checklist and allocation of responsibilities

Contact	Responsibilities
Legal Gilbert Ducasse General Counsel Phone: 03) 9479 1795	- Provide advice on the extent and cause of the breach and the potential harm; - Provide advice as to which individuals or organisations are required to be notified; and - Provide advice on legal, contractual or insurance obligations which may arise.
ICT David Hird Head, Security Standards & Compliance Phone: 03) 9479 3979	- Contain (if possible) the breach and prevent additional information loss; - Start forensic examination into the source, and extent, of the breach; and - Implement measures to prevent further data breaches.
Privacy Officer Fiona Rowley FOI & Privacy Officer Phone: 03) 9479 1839	- Liaise with Legal and ICT to determine the extent of the breach; and - Prepare the relevant statement for: o Commissioners Officer and other external stakeholders
Risk Management	- Assess the risks from the breach; - Review and provide advice on the actions to prevent a further data breach.
Communications	- Assist in communicating with affected individuals and dealing with the media.

Regulatory

Commissioner for Privacy and Data Protection (Victoria) – www.cpda.vic.gov.au

Office of the Australian Information Commissioner (Commonwealth) - www.oaic.gov.au