



Data Breach Response Process Flowchart

MAINTAIN INFORMATION SECURITY – APP 11

Protect information from misuse, interference and loss, from unauthorised access, modification or disclosure. To comply with their obligations under the APPs, the School’s MNDB Management Team (MNDBMT) should consider:

- the sensitivity of the personal information
- the harm likely to flow from a security breach
- developing a compliance and monitoring plan, and
- regularly reviewing the School’s information security measures.



DATA BREACH OCCURS

Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference.



KEY STEPS IN RESPONDING TO A DATA BREACH

Step 1	Contain the breach and make a preliminary assessment	<ul style="list-style-type: none"> • Take immediate steps to contain breach • Designate person / team to coordinate response (MNDBMT)
Step 2	Evaluate the risks for individuals associated with the breach	<ul style="list-style-type: none"> • Consider what personal information is involved • Determine whether the context of the information is important • Establish the cause and extent of the breach • Identify what is the risk of harm
Step 3	Consider breach notification	<ul style="list-style-type: none"> • Risk analysis on a case-by-case basis • Not all breaches necessarily warrant notification



SHOULD AFFECTED INDIVIDUALS BE NOTIFIED?

Where there is a real risk of serious harm, notification may enable individuals to take steps to avoid or mitigate harm.

Consider:

- Legal / contractual obligations to notify
- Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities)

Process of Notification

- When? – as soon as possible
- How? – direct contact preferred (mail / phone / email)
- Who? – entity with the direct relationship with the affected individual – the Head of School and / or the Head of Finance and Business Services
- What? – description of breach, type of personal information involved, steps to help mitigate, contact details for information and assistance.



SHOULD OTHERS BE NOTIFIED?

- Office of the Australian Information Commissioner (OAIC)
- Police / Law Enforcement
- Professional or Regulatory Bodies
- Other agencies or organisations affected by the breach or contractually required to notify



- Step 4 Review the incident and take action to prevent future breaches
- Fully investigate the cause of the breach
 - Consider developing a prevention plan
 - Option of audit to ensure plan implemented
 - Update security / response plan
 - Make appropriate changes to policies and procedures
 - Revise staff training practices

