8. Notifiable Data Breach Procedure

Policy

Intellectual Copyright

It is a condition of GSA as an incorporated status the organisation will follow this policy and procedure keeping the best interest of the graduates, staff and other stakeholders involved.

Procedure

Assessing a suspected notifiable data breach (NDB)

If a GSA staff member has reason to suspect that there may have been a data breach, they are required to notify the Manager and/or the CEO of the suspected breach.

The CEO/ Manager needs to move quickly and assess whether an eligible data breach has occurred and where possible immediately contain the suspected or known breach. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information. If it is determined, there are reasonable grounds to suspect that there may have been a serious breach; the Australian Information Commissioner (AIC) must be notified.

The CEO must take all reasonable steps to complete the assessment within 30 calendar days after the day the suspected breach was identified. Where possible the assessment should be completed in a shorter time.

The assessment follows a three-stage process:

1. **Initiate:** decide whether an assessment is necessary and identify which person or group will be responsible for completing it

2. **Investigate:** quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts, and

3. **Evaluate:** make a decision, based on the investigation, about whether the identified breach is an eligible data breach.

The assessment process should be documented and retained.

The following link should be used to guide and inform the assessment process. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches

An eligible data breach occurs when the following criteria are met:

•There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).

•This is likely to result in serious harm to any of the individuals to whom the information relates.

•The entity has been unable to prevent the likely risk of serious harm with remedial action.

At any time, including during an assessment, GSA will take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. If remedial action is successful in preventing serious harm to affected individuals, notification is not required.

2. An eligible data breach has occurred

- GSA will notify the affected individuals about the eligible data breach.
- GSA will prepare a statement and provide a copy to the Australian Information Commissioner.
- GSA will use the Office of the Australian Information Commissioner's (OAIC) online form to inform and complete the statement. https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

The statement will include the name and contact details of the entity, a description of the eligible data breach, the kind or kinds of information involved, and what steps the entity recommends that individuals at risk of serious harm take in response to the eligible data breach.

GSA will notify affected individuals about the contents of this statement or, if this is not practicable, publish a copy of the statement on the website and take reasonable steps to publicise the contents of the statement.

Responsibility

The GSA Board is responsible for adopting this policy.

The GSA Board members, Council Members, Chief Executive Officer and all staff members, contractors and volunteers are responsible for the implementation of this policy.

Supporting Documents

- Employee Agreement
- Code of Ethics and Conduct
- Privacy Policy
- Email Policy