REPORTING A PRIVACY/DATA BREACH

1. What is a Privacy/Data Breach?

A privacy or data breach happens when confidential, sensitive or protected data, including personal information, is accessed, copied, transmitted, viewed, stolen or used by an individual unauthorised to do so, e.g.:

- Someone's personal information is sent to the wrong person
- A database containing confidential information or research data is hacked
- An unencrypted and unlocked laptop or external hard drive goes missing
- A third party vendor supplying hosting, data processing or other technology services notifies of data breach
- Loss of hardcopy information that contains confidential information

2. What do I do if I think there has been a Privacy/Data Breach?

ACT FAST: THE FIRST 24 HOURS FOLLOWING A BREACH ARE CRITICAL

Report

Provide as much information as possible, including:

- · The time and date the suspected breach occurred
- · when it was discovered
- · The types of data involved, including the type of personal data
- · the affected cohort e.. staff, students, other
- · The cause and extent of the breach
- · any immediate containment action that has occurred

Contain

If possible, immediately contain the breach e.g.

Team by emailing: privacyalert@griffith.edu.au

- · Remotely disable the lost device
- Recall the email from the recipient
- contact the recipient and ask them recipient not to read and to delete the email/arrange for collection/return of the posted materials.

If you become aware of a data breach (or are unsure as to whether a

data breach has occurred), report immediately to the Privacy Alert

If immediate containment is not possible, stop - do not try to fix it yourself.

Preserve

Preserve any evidence, including details of:

- · the exact time of the incident;
- · any other person/s who witnessed the incident;
- · copies of any emails or file notes relating to the incident.

Further help or advice can be found by contacting the Privacy Officer: privacy@griffith.edu.au