

Privacy Event Response Protocol

A privacy event is an incident where personal information in the custody or control of the University, is treated in a manner that is not in accordance with FIPPA, e.g. e-mailing personal information to the wrong person, loss of unencrypted devices containing personal information.

How Should You Respond When a Privacy Event Happens?

Immediately report any privacy event or possible privacy event to your manager, Divisional Freedom of Information Liaison (FOIL) and/or FIPP Office. If uncertain, report the matter to ensure that no privacy events are missed.

Consult with the above officials, who will guide you through the following steps to quickly and effectively address the privacy event.

Assess the extent of the privacy event, e.g. is it a one-time occurrence, potentially repeatable or an on-going problem; list and describe individuals affected including the number of individuals; what was the cause and likely scope of the privacy event; what fields of personal information types are involved, e.g. name, address, e-mail address, student number, grades; what medium is involved, e.g. hard copy, electronic, verbal.

Contain the privacy event immediately by taking remedial action, e.g. stop process/activity that caused the privacy event; make arrangements to retrieve records; take applications off-line. Determine the effect of the remediation steps and identify any remaining issues/gaps.

Document the details of the privacy event, i.e. date, time, location of the privacy event; which faculty/department etc. is affected; how was the privacy event discovered; when was the privacy event reported and to whom. Document any other pertinent information such as how was the personal information protected, e.g. locks, alarm system, passwords, encryption.

Brief University officials on the privacy event and how it is being managed, as appropriate. Document names/titles and date/time of briefings.

Notify the individuals whose personal information was affected by the privacy event, except where notice is not appropriate or possible. Examples for not notifying affected individuals includes: identities of affected individuals are unknown; contact information is unavailable; notice would interfere with a law enforcement investigation etc. List who was/will be notified and keep a copy of the notice.

What Should You Do to Prevent Future Privacy Events?

Analyze the events leading to the privacy event.

Evaluate what was done to contain the privacy event.

Identify what needs to be done to prevent future privacy events.

Implement measures to prevent future privacy events, e.g. project redesign, staff training, access controls, secure destruction procedures etc.