PRIVACY BREACH NOTIFICATION PROCEDURE

PURPOSE

The purpose of this document is to provide instructions to members of the University community on how to respond to a breach of privacy in compliance with the University's Access to Information and Protection of Privacy Policy ("Access and Privacy Policy").

PART A

What is considered a breach of privacy

A privacy breach occurs when personal information (PI) is disclosed in contravention of the *Freedom of Information and Protection of Privacy Act ("FIPPA")*. For example, the personal information may be:

- Lost (e.g. a file containing personal information is misplaced within the University),
- Stolen (e.g. a laptop containing personal information is stolen), or
- Inadvertently disclosed through human error (e.g. a letter addressed to person A which contains personal information is actually mailed to person B).

PART B

What to do if a privacy breach is suspected or confirmed

If you suspect that an individual's personal information has been breached, you should immediately:

1. **Contain**
   You should take immediate steps to contain the breach. For example:
   - If Personal Information was inadvertently disclosed to another individual, retrieve the hard copies of the Personal Information that was disclosed, ensure that no copies of the Personal Information have been made or retained by the individual and obtain the individual's contact information in the event that follow-up is required.
   - Determine whether the privacy breach would allow unauthorized access to any other Personal Information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change

passwords, identification numbers and/or temporarily shut down a system).

2. **Immediately inform:**
   - Your Unit Head, and
   - Unit Head is to inform the University's Freedom of Information and Privacy Coordinator ("FIPPA Coordinator") at 905-688-5550, ext. 5380, or by email.

3. **Complete Privacy Breach Report Form**
   To document the breach, aid in the investigation, and corrective action:
   - Complete Steps 1 & 2 of the Privacy Breach Report Form.
   - Provide a copy of the Privacy Breach Report Form to your Unit Head, and the FIPPA Coordinator.
   - FIPPA Coordinator to complete Steps 3 & 4 of the Privacy Breach Report Form.

PART C

How the University will respond to a privacy breach

The Privacy Breach Report Form will guide you through the steps to be completed for each suspected privacy breach. Here is a summary of each step within the Privacy Breach Report Form, as follows:

Step:

1. **Contain**
   The FIPPA Coordinator will work with you and your Unit Head to ensure the breach is contained.

2. **Assess the Risks**
   You should assess the types of Personal Information involved and the sensitivity of the information breached to determine the appropriate response and notification to affected individuals. Examine the situation fully and work with the FIPPA Coordinator to ensure that any necessary details of the breach and any corrective actions are documented for later investigation and review.

   Assess the cause and extent of the breach, as well as the foreseeable harm from the breach (e.g. identity theft, damage to the individual's or University's reputation).

3. **Notify Affected Individuals**
   Identify those individuals whose privacy was breached and inform the FIPPA Coordinator. The FIPPA Coordinator will

determine what form of notification is appropriate, with advice from the University's General Counsel.

4. **Investigate and Correct**
   The FIPPA Coordinator will further investigate the cause of the privacy breach, work with the unit concerned to prepare documentation and consider whether to develop a prevention plan. A prevention plan may address such issues as employee training, policy review or development, audit of physical and/or technical security, and a process to ensure that the prevention plan has been fully implemented.

Decisions on how to respond to a suspected or confirmed privacy breach will be made by the General Counsel on a case by case basis, based on advice from the FIPPA Coordinator. The University will take each situation seriously.

General Counsel, in consultation with Senior Administration, will determine whether Ontario's Information and Privacy Commissioner (IPC) should be notified of the breach.

October 15, 2015