Procedure: Privacy Breach Notification

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to all Ontario Universities and establishes requirements in order to protect individuals' privacy regarding the collection, use, disclosure, retention, disposal and security of personal information.

The purpose of this procedure is to outline the action to be taken in the case of a privacy breach. A privacy breach is defined as any incident involving unauthorized or inappropriate disclosure of personal information.

DEFINITION OF PERSONAL INFORMATION

Personal Information, as defined by FIPPA, means recorded information about an identifiable individual, including, but is not limited to such basic details as name, home address, telephone number, gender, age and marital or family status, race, national or ethnic origin, colour, religious or political affiliations, employee history, employee number, student number, health information, educational history, disabilities, blood type, financial history, criminal history, other persons' opinions about an individual, an individual's private views or opinions, and name, address and phone number of parent, guardian, spouse or next of kin.

Personal information does not include the name, title, business address, and business contact numbers of an employee.

RESPONSIBILITIES

Under FIPPA, all Brock employees who handle or manage personal information on behalf of the University have a responsibility to ensure that the information remains confidential and secure. The protection of personal information should be integrated into programs, services, and systems on a proactive basis.

PROCEDURE

If a privacy breach is suspected or confirmed, report this to your immediate supervisor (or, if unavailable, the next available level of management). Your supervisor is to gather the details and then immediately contact the Freedom of Information and Privacy Office at 905-688-5550, ext. 5380. The Freedom of Information and Privacy Office will discuss the immediate steps to be taken in order to mitigate the negative impact of a breach and work to prevent further inappropriate disclosures of personal information.

All privacy breaches are taken seriously and will be investigated by the Freedom of Information and Privacy Office. If a breach is confirmed, the Freedom of Information and Privacy Office will notify all other pertinent parties and may commence an internal investigation.

Based on the results of the assessment by the Freedom of Information and Privacy Office, consultations will occur with the appropriate Senior Administrator(s) regarding the necessary steps to be taken. The Freedom of Information and Privacy Office follows the Information Privacy Commissioner's guidelines of actions the University should follow if a privacy breach occurs.

INVESTIGATE AND CORRECT

Senior Administration may recommend a further investigation into the cause of the privacy breach, and work with the unit concerned to develop a prevention plan. The 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.

RELATED POLICIES

- Access to Information and Protection of Privacy Policy
- Access to Student Records and Disclosure of Information Policy

For more information about the application of these procedures, please see Brock University's Freedom of Information and Protection of Privacy website at www.brocku.ca/university-secretariat/freedom-information-protection-privacy or contact the Freedom of Information and Privacy Coordinator at 905-688-5550, ext. 5380.

Dated: February 14, 2011