Privacy Guidelines – New College, University of Toronto

Access to information

New College Faculty and Staff have access to a range of confidential information. At the University, information which is not intended to be public is confidential. One key type of confidential information is personal information, which is information about an identifiable individual. A University employee is permitted to access only personal information required to fulfill official University job responsibilities. Information must not be released to or discussed with anyone other than the individual whose information is involved, or other University staff who need the information to fulfill their official duties, or unless the individual has given explicit consent. One of our key responsibilities is to ensure that the personal information of students and others we deal with is kept confidential and secure.

Following are required practices that will help ensure we meet this obligation. If you have any questions or special requirements with regard to these issues, please feel free to discuss them with your manager or director.

Further information is provided in **Access and Privacy Practices: General and Administrative:**

www.provost.utoronto.ca/Assets/Provost+Digital+Assets/Provost/Provost+Digital+Assets/Provost/fippa.pdf

Electronic information

1. Confidential information, including personal information (such as names, student numbers, contact information, academic information, financial information, etc.) should not be stored on local devices (e.g. your computer's hard drive or a USB key). This information should be held in a secure institutional database (ROSI, StarRez, DIS, etc.) or on private network drives. If there is an exceptional circumstance requiring local storage, the device and file must be encrypted.

2. Personal information should not be transported outside the office, whether on a laptop or portable storage device such as a USB key, or kept on a home computer. Because of the sensitivity of this information, this is the case even when the information is encrypted. Any exceptions must be approved in advance by a manager or director, and the approval documented.

3. Mobile devices, including laptops, smartphones, tablets and other devices which store confidential information, including university email, must be encrypted. This is true whether they are University or personal devices. Unencrypted personal devices must not be used to access University email or other confidential University information.

4. With the exception of internal email (from one UTOR address to another UTOR address), email is not a secure form of communication. Use of email to share personal information should be limited to cases when there are no reasonable alternatives, and information shared in this way should not include any sensitive data.

5. Email containing personal information should be kept for one year. Other email should be deleted/destroyed as soon as it is no longer required.

6. Confidential information in electronic form should be securely destroyed at the end of all applicable retention periods.

Paper documents

1. Just as with electronic information, paper documents and files containing personal information are highly confidential. These should be placed in locked cabinets overnight or during absences from the office, and office doors should be locked. This follows the principle of protecting documents behind two levels of locks – one on the building and/or office, and another inside a cabinet.

2. Great care should be exercised in transporting paper documents outside the office. This should only be done when absolutely necessary and with the knowledge and permission of your Director or Manager. If you must take files home, take as few at a time as possible, take copies rather than originals, and ensure they are always with you during transit. Any confidential and/or personal information that is taken home must be locked when not in use.

3. Whenever possible confidential information should be managed electronically and housed on secured servers. The College will develop a standard operating procedure for dealing with such information in paper form.

4. Always use a cross-cut shredder to destroy paper records or dispose in the shredding disposal consoles provided by the College.

Clean desk policy

1. When leaving your office, ensure that confidential documents, including documents with personal information, are locked in a cabinet or drawer.

Parents and third parties

1. We often receive requests from parents or other third parties for access to student information; these individuals may be very persistent in their inquiries. Parents do not have a right to such information; in fact, privacy legislation explicitly prevents us from sharing any personal information with a third party unless the individual (e.g., the student) has consented. If you are sharing student information with a parent, please have written authorization from the student, or have the student present at the time of sharing.

Emergency situations

1. We have an obligation to provide personal information in compelling circumstances that affect the health or safety of an individual, where providing that information would help. Safety trumps privacy. Consult your Manager or Director whenever there is a health or safety concern, and be sure that you follow the University's Emergency Disclosure of Personal Information guideline:

   http://www.hrandequity.utoronto.ca/about-hr-equity/news/memo/2008_-_2009/Memo_2008-09_HR16.htm

Loss of information

1. If any personal information is lost or misplaced, e.g., a document, file, USB key, laptop, etc., we have an obligation to report this to the FIPPA office. In such cases, please notify your Director or Manager immediately. Often the consequences can be minimized with quick intervention.