Access and Privacy Practices:

General and Administrative

June 23, 2011

These practices support privacy protection and sound record handling consistent with the *Freedom of Information and Protection of Privacy Act* (FIPPA).

FIPPA applies to ALL RECORDS in the custody or under the control of the University.

FIPPA creates a public right to request records from institutions like the University. Some, such as records associated with research, may be protected from disclosure.

FIPPA protects individual privacy by regulating University actions involving personal information, including how it is collected, used and disclosed.

Employment and labour relations records are excluded from FIPPA coverage but must always receive full privacy protection because of the sensitive information they contain.

This document sets out practices for:

1. Collection of personal information
2. Use or disclosure of personal information
3. Retention of personal information
4. Types of information
5. Security for personal and other confidential information
6. Clean desk
7. Secure destruction
8. Privacy event responses
9. Records management
10. Recording Meetings
11. Privacy and Access/Records Management Tips

Section One sets out key definitions, principles and a brief summary of the practices.

Section Two contains the complete practices.

These practices apply to all University administrative and operational records. Take particular care with records which contain personal or other confidential information.

For questions or assistance, please contact the Freedom of Information and Protection of Privacy (FIPP) Office at (416) 946-7303 or (416) 946-5835.

Section One

Definitions

Personal information is information about an identifiable individual or that identifies an individual, e.g. home or email address, student number, grades etc. Personal information does not include information about someone acting in a business or professional capacity, e.g. University employee name, position and work records are not usually personal information.

Confidential information is information intended for limited distribution and not to be generally or publicly available, e.g. HR records, non-public financial information etc.

Principles and Summary of Practices

Informational privacy is the principle that individuals should have control over their personal information, to an extent consistent with law and institutional activities.

Individuals should be notified in advance how their personal information will be handled.

1. Collection of personal information

Only collect personal information as necessary for established University functions. Collect the minimum amount of personal information needed to accomplish the function.

The University must have legal authority to collect personal information. This means:

a. Collection is expressly authorized by statute (e.g. University of Toronto Act), or
b. The personal information is to be used for purposes of law enforcement, or
c. Collection is necessary for the proper administration of a lawfully authorized activity.

A Notice of Collection is needed when collecting personal information, including:

a. The legal authority for the collection of the information,
b. The principal purpose(s) for which the information is intended to be used, and
c. Title, business address and phone number of a university official to answer questions.

Collect personal information directly from the individual to whom it pertains. Consult the FIPP Office if personal information needs to be collected for other purposes. Personal information generally cannot be collected indirectly (from someone else) without an individual's consent.

2. Use or disclosure of personal information

Only use personal information for purpose(s) for which it was collected, for a consistent purpose, or with consent of the individual. A purpose is consistent if the use is "reasonably compatible" with a purpose given on collection or in a Notice of Collection.

Do not disclose personal information except in limited situations such as:

- Consent of the individual to whom the information pertains;

- Disclosure for purpose(s) for which the personal information was collected;

- Need-to-know; to a University employee, officer, agent or contractor who needs the information to perform official, proper University duties;

- Externally **only** as required by law, established University practice or policy;

- In compelling circumstances affecting the health or safety of an individual;

- In compassionate circumstances to facilitate contact with the spouse, close relative or friend of an individual who is injured, ill or deceased.

Limit availability of personal and other confidential information to legally and operationally entitled individuals, programs and offices.

3. Retention of personal information

Retain personal information for at least one year after its last use unless the person to whom it pertains consents to earlier disposal. This provides a reasonable window of time for individuals to access their own personal information or challenge official actions. University record retention requirements may necessitate that the information be kept longer than one year. Take reasonable steps to ensure that personal information is not used unless it is accurate and up-to-date.

4. Types of information

Understand the varying requirements for different information types at work, including privacy of personal information and confidentiality of other sensitive information.

5. Security for personal and other confidential information

Privacy is an overarching institutional responsibility shared by all at the University. Staff and faculty should protect personal and confidential information from unauthorized access and unintended destruction, e.g. locked filing cabinets, password protection, fully encrypted laptops and USB memory sticks.

Privacy and confidentiality must be supported with strong security; technical, physical and administrative measures that protect information through its lifecycle, from creation or collection to disposal. Use security measures appropriate for the information protected to minimize the possibility of unauthorized access as much as you reasonably can.

Only remove electronic or hard copy records that contain personal and other confidential information from a secure institutional environment if you keep them secure, you have official authorization, operational need and no other reasonable means to do the task.

6. Clean desk

Faculty and staff must secure personal and confidential information when not at their work area, e.g. at breaks or meetings. Keep personal or confidential information securely locked including using passwords to access computers. Before leaving for the day, secure your workspace, IT resources and information to prevent unauthorized access.

7. Secure destruction

At the end of their lifecycle, University records should be sent to University Archives or disposed of. Records of personal or confidential information must be securely destroyed.

Personal or confidential information should be made irretrievable. Crosscut shred paper records; cut CDs and DVDs into small pieces; repeatedly overwrite computer drives with “junk” data before disposal or return to lease companies.

8. Privacy event response

Immediately report all possible privacy issues, such as inappropriate disclosure of personal information, to your supervisor, your Division’s Freedom of Information Liaison (FOIL) or the FIPP Office. This supports a quick and effective response. If uncertain, always report.

9. Records management

Like other assets, manage University information and records to maximize their usefulness for University operations. Only create records needed for your work. Include all necessary information but nothing that is irrelevant. Follow University records management standards and practices, including records retention schedules.

Preserve official records needed for University business or to document actions taken. Delete transitory records, such as rough notes, drafts, copies and personal messages.

10. Recording meetings

Meeting records should capture only information needed to achieve meeting objectives.

Establish meeting record parameters (recorder, format, content of official record, publication dates, etc.). Establish how personal or confidential information discussed at the meeting will be protected. Avoid creation of unofficial, “alternative” meeting records.

11. Privacy and Access/Records Management Tips

These are brief reminders of key privacy, access and records management principles.

Section Two: Practices

Collection of Personal Information

Purpose and Objective

This practice guides the University's collection of personal information.

Checklist

☐ 1. Collect personal information only if needed for established University functions.

☐ 2. Collect the minimum amount of personal information **needed** for the activity.

☐ 3. The University cannot legally collect personal information unless:
   a. Expressly authorized by statute (e.g. University of Toronto Act), or
   b. Used for the purposes of law enforcement, or
   c. Necessary for the proper administration of a lawfully authorized activity.

☐ 4. Collect personal information directly from the person to whom it pertains, unless:
   a. He or she consents to collection from someone else, or
   b. To determine suitability for an honour or award, or
   c. To recognize outstanding achievement or distinguished service, or
   d. To conduct a proceeding or possible proceeding before a court or tribunal, or
   e. For law enforcement purposes.

☐ 5. Provide a Notice of Collection containing:
   a. The legal authority for the collection of the information,
   b. The principal purposes for which the information is intended to be used, and
   c. Title, address and phone no. of a University official to address questions.

Background

The University "collects" whenever it acquires, gathers or receives personal information.

Student personal information can be collected if needed for official activities such as registration, grading, granting degrees, discipline, program assessment and where sharing of personal information is part of a program activity. Personal information can also be collected for purposes central to students' university experience, like athletic activities.

For optional purposes, like recreational activities, student directories and clubs, student opt-in is usually necessary. In such cases, or if uncertain, clarify with the FIPP Office.

Collecting personal information directly from an individual helps him or her to know and control how the University uses the information. Check with the FIPP Office before collecting personal information from a source other than the individual.

The University uses a Notice of Collection to inform individuals of University purposes for personal information and to define allowable uses and disclosures by the University.

A Notice of Collection for most University activities has been posted to ROSI and is included in calendars. It reads as follows:

The University of Toronto respects your privacy. Personal information that you provide to the University is collected pursuant to section 2(14) of the University of Toronto Act, 1971. It is collected for the purpose of administering admissions, registration, academic programs, university-related student activities, activities of student societies, safety, financial assistance and awards, graduation and university advancement, and reporting to government agencies for statistical purposes. At all times it will be protected in accordance with the *Freedom of Information and Protection of Privacy Act*. If you have questions, please refer to www.utoronto.ca/privacy or contact the University Freedom of Information and Protection of Privacy Coordinator at 416-946-7303, McMurrich Building, room 104, 12 Queen's Park Crescent West, Toronto, ON, M5S 1A8.

For some activities, it may be necessary to add to or customize the above Notice. The FIPP Office can help you to determine the need for a notice or customization.

Notices of Collection are generally given in writing on a form or website but can be given in any manner that ensures the individual has been notified, e.g. a Notice can be:

1. Spoken or read to an individual on the telephone or at a service desk or office.

A precise “script” ensures consistency when notice is given verbally. You should create a written record that the Notice was read to and understood by the caller.

2. Prominently posted where collection occurs.

A Notice can be printed on a form or on a sign notifying, for example, video security.

Use or Disclosure of Personal Information

Purpose and Objective

This practice Guides the use and disclosure of personal information within and outside the University.

Checklist

☐ 1. Use and disclose personal information only for the purpose for which it was collected, for established University functions, or with consent of the individual.

☐ 2. Share personal information within the University only on a need-to-know basis:

Only disclose personal information to a University officer, employee, consultant or agent if they need the record in the performance of his/her duties and disclosure is necessary and proper in the discharge of the University's functions, e.g. don't respond to an email with Reply To All if only one individual has a need-to-know.

☐ 3. Even when there is a need-to-know, be cautious about faxing or emailing personal information and about leaving confidential information on a voice message.

☐ 4. Know which uses/disclosures of personal information **are** and are **not** permitted in your work.

☐ 5. To avoid inadvertent disclosure of personal information, do not include information about identifiable individuals unnecessarily in documents, emails etc.

Background

University practices provide for the use or disclosure of personal information only for established University purposes. Uses and disclosures of personal information should be:

1. Consistent with the purposes listed in University Notices of Collection,
2. Necessary to accomplish the (established University) purposes,
3. Consistent with faculty/program/divisional/University practices and activities.

When uncertain whether a use or disclosure of personal information is permitted, contact your FOIL or the FIPP Office.

Consent

Personal information may be used or disclosed with consent from the individual to whom the information pertains. Obtain written consent indicating:

- The particular personal information to be used/disclosed,
- The use being consented to or the entity to whom the information is to be disclosed,
- The date of the consent.

Where consent to use or disclose is obtained verbally, document it and ideally confirm through correspondence with the individual, indicating the above three points.

Where an individual purports to act as an agent for someone, the University has an obligation to verify whether or not the agent is properly authorized to obtain such information. Take special care where personal information is particularly sensitive, e.g. student grades. In such cases, contact the individual to whom the information relates to verify the status of his/her agent.

Purpose or Consistent Purpose

Personal information may be used or disclosed for the purpose(s) for which it was collected or for consistent purposes. A consistent purpose is one which: might reasonably have been expected at the time of collection; is "reasonably compatible" with the purpose for which the personal information was collected by the University; or consistent with the purpose(s) listed in the Notice of Collection. Contact the FIPP Office if uncertain. If a needed use or disclosure of personal information is not included in the Notice of Collection, contact the FIPP Office to discuss customization of the Notice.

Need-to-Know Disclosure -- For disclosures within the University

Personal information may be disclosed as necessary within the University on a need-to-know basis according to the “Need-to-Know Principle”, which provides that:

Personal information may be provided to a University officer, employee, agent or consultant, who needs the personal information for the performance of his/her duties, if the disclosure is necessary and proper in the discharge of the University's functions. Personal information should be disclosed to agents or consultants only with a confidentiality agreement and/or having privacy protection built into the contract.

Responsibility for the need-to-know principle rests with the entire University. Both a University official seeking the personal information and an official who may disclose it are responsible for ensuring that the disclosure is proper. For example, an employee responsible for student data and a professor who requests the data are jointly responsible for following the need-to-know principle. The professor should only request personal information needed for the performance of duties, where the disclosure is necessary and proper for University functions. The employee must only release this specific personal information to a University official who is known to need it for proper purposes.

Need-to-know applies to required personal information in a document or record, but not necessarily to the entire document. Rather than sharing entire records or files, provide only the specific information needed by the individual making the request.

Need-to-know operates only within the University. Disclosures of personal information outside the University must conform to established University practice. If unsure, consult practices, policies, your supervisor or the FIPP Office.

Law Enforcement Disclosure

Personal information may be disclosed to a law enforcement agency such as a police force, to aid a law enforcement investigation. However, the University may choose to require a warrant, summons or court order before such a disclosure. Except for emergency situations, always check law enforcement disclosures with University of Toronto Campus Community Police, the FIPP Office or University legal counsel.

Compelling Circumstances Disclosure

The University should disclose personal information in compelling circumstances, where delay in sharing information could impact health or safety, e.g. disclosure of personal information to health care providers and/or family to help a distressed individual or to prevent a suicide. Try to consult with your manager or other appropriate University officials but you should act if you can't contact them. **Safety always takes precedence.**

Immediately contact emergency response services or police where there is apparent or imminent injury, threat, danger or violence.

Compassionate Circumstances Disclosure

The University may contact next-of-kin or a friend to inform them of injury, illness, or death. Personal information may be disclosed about the injured or deceased person to the relative or friend. Only personal information necessary to facilitate contact should be disclosed and the FIPP Office should be consulted prior to such disclosures.

Uses and Disclosures to Avoid

Do not use or disclose personal information where it is merely convenient or desirable. For example, a software contractor need not see personal data, where depersonalized information could be used. Never compromise privacy for administrative convenience.

Avoid:

Emailing or faxing personal information or leaving confidential information on a voice mail message,

Sharing personal information with everyone in your workplace,

Revealing personal information in a public setting while on your cell phone.

Retention of Personal Information

Purpose and Objective

This practice explains the need to retain personal information for at least one year after its last use unless the individual to whom it pertains consents to its earlier destruction.

Checklist

☐ 1. Know what personal information is contained in records with which you work.

☐ 2. Follow University retention schedules and requirements applicable to your records.

☐ 3. Retain personal information for at least one year after its last use.

Background

All University offices should follow retention requirements for its records. Information of identifiable individuals must be retained for at least one year after the date of its last use. Record retention schedules are often longer to meet business, fiscal or legal requirements.

You need not retain personal information in the form that it was received, e.g. feel free to transcribe voice mail or print out and retain a hard copy of an e-mail.

For FIPPA access requests, retain all records until the matter is complete and all appeal periods have expired.

Do not destroy personal information less than one year after its last use unless you have the documented voluntary consent of the individual to whom it pertains.

Types of Information

Purpose and Objective

The University holds many types of information that require protection, such as student records, teaching materials and research data. This practice lists some major information categories and guidance for their handling.

Checklist

☐ 1. Understand different information types and their requirements.

☐ 2. Follow legal requirements, University policy and practice.

☐ 3. Understand and follow correspondence confidentiality standards.

Background

Personal Health Information

Personal health information (PHI) is defined in the *Personal Health Information Protection Act* (PHIPA) to include identifying information about an individual that relates to health, health history, providing of health care, health number and other related data. PHIPA sets out detailed standards for privacy and access of PHI, including consent requirements for sharing PHI.

Personal Information

Personal information is defined in the *Freedom of Information and Protection of Privacy Act* (FIPPA) as recorded information about an identifiable individual. FIPPA contains rules for the collection, use, disclosure, retention and destruction of personal information.

Third Party Commercial Information

FIPPA protects some types of third party information, such as commercial information supplied to the University in confidence, where disclosure can reasonably be expected to result in specified harms to the third party.

Solicitor-Client Privileged Information

Legal advice and solicitors' records for use in litigation are protected under FIPPA and at common law if they are kept confidential between the solicitor and client.

Research and Teaching Materials

Research and teaching materials are not covered by FIPPA and not disclosed in response to access requests. They are not disclosed outside the University, nor shared within the University without a need-to-know. Protecting these materials is very important.

Information Protected By Policy

Policies may set out requirements for information to be kept confidential. There are many examples, such as policies respecting student academic records or academic appeals.

Information Protected By Practice

Practice dictates that some records **not** be disclosed, even if they might later be found to be publicly releasable. For example, operational planning records might not be disclosed without careful assessment of possible harm to individuals, to the University or to other parties such as contractual partners or bidders in procurement situations.

Confidentiality is expected for various types of information, having to do with many topics, such as business, intellectual property or labour relations.

Correspondence

Correspondence includes letters, faxes, e-mail, text messages and other written or recorded communication which can be sent and received. Correspondence is addressed to a recipient(s) who may be identified in any of a number of ways, such as;

- A named individual, with or without a position or title
- A position, title or office, without a name
- A group or list of named individuals
- A group or list of positions or offices
- A category of individuals, such as all system administrators
- All individuals within a unit or an organization

Correspondence confidentiality varies according to how it is marked as follows:

Confidential

Correspondence marked confidential is intended for the office or unit to which it is addressed and must only be opened by that office or unit. These communications are often operational and meant to be opened by those who process records at the destination such as the individual to whom it is addressed and other supporting staff at that office.

(Strictly)Personal and Confidential, Private and Confidential, Addressee (or Recipient) Only

This type of correspondence is intended only for the individual whose name it bears and not to be opened by anyone else. An exception is correspondence to an executive such as a Vice-President, which can be opened by an assistant who is authorized to open it. Correspondence marked this way can relate to important or sensitive matters and should be protected from unauthorized access.

No Specific Marking

Treat correspondence that is not specifically marked as personal and/or confidential, particularly if the origin or addressee suggests sensitive or confidential information in the context of an office's operations. Such correspondence should be protected from distribution beyond intended recipient(s).

Standards

Different information types need to be treated differently regarding access, sharing and security. There is a spectrum, ranging from information intended for public dissemination to information intended only for one specific individual:

Public Information - available to all without restrictions, such as material posted on websites like governance reports, course descriptions and news releases.

Internal Circulation - information that is available within an organization, perhaps on an intranet site. It might be released on request, but is not public and must be reviewed to prevent disclosure that is inconsistent with legal or administrative requirements.

Defined Group - information restricted to a group of individuals, who have a need-to-know (e.g. student personal information) to accomplish their work.

Individual - information intended for a specific individual only and not shared without the individual's consent, e.g. correspondence marked "personal and confidential".

Security for Personal and Other Confidential Information

Purpose and Objective

Law, policy and practice require that personal, health and other confidential information, be protected from unauthorized access.

This practice supports protection of electronic and hard copy records, consistent with law, policy and risk management practice. It does not supersede University IT security standards or measures such as those under the Chief Information Officer, but is intended to work with them.

The objective is to protect confidential information from unauthorized access, without disrupting University operations, and with measures appropriate for each type of record.

Checklist

☐ 1. Know which records in your work are confidential and require protection; e.g. records that contain personal or health information.

☐ 2. Keep hard copy confidential records in a secure institutional environment; locked in a non-public area when not in use or you are not present.

☐ 3. Keep electronic records of confidential information in a secure server environment.

☐ 4. Only take confidential records out of secure environments if you have: official authorization; operational need; and no other reasonable means to accomplish the task.

☐ 5. Only take hard copy confidential records out of a secure institutional environment, as necessary for immediate work. Protect them with strong security, including keeping records out of sight, secure lockup and other security measures offsite and at home.

☐ 6. To take confidential electronic records out of a secure server environment, encrypt your drive, memory stick or mobile device with the latest version of commercially available and supported encryption software, or de-identify the information.

☐ 7. When work permits, use depersonalized records, not personally identifiable ones.

☐ 8. Access confidential electronic records remotely using encrypted secure means such as virtual private network or encrypted remote desktop connection.

☐ 9. Encrypt attachments that contain personal or confidential information to email them to non utoronto.ca addresses. Communicate passwords by phone, not by email. Do not email or forward unencrypted personal or confidential information out of the utoronto.ca email system because it could be viewed by third parties if intercepted.

Background

In the performance of its duties, the University collects, uses and discloses personal information, including home email addresses, student records and grades. Individuals expect their privacy to be respected and the University is legally required to protect all personally identifiable information with strong security.

Treat all information in your work at the University as confidential and protected unless your work requires you to make it publicly available.

Examples of confidential information include:

Personal Health Information
Third Party Commercial Information
Solicitor-Client Privileged Information
Research or Teaching Materials
Information Protected by Policy or Practice, e.g. HR data, non-public financial information
Records in draft form or in development that are not finalized or approved.

Understand which information in your work is confidential. This context results from an office's role, operations and relationships and should be clear to managers and staff. If you have any doubt about confidentiality expectations, consult within your office.

Do not take confidential hard copy or electronic records away from secure institutional and secure server environments, e.g. home for work, unless you have official authorization and operational need and no other reasonable means to do your work.

Official Authorization - There is official University, Division or department policy or practice that permits the record to be taken out. If there is any doubt, consult with the unit manager.

Operational need - The record must be taken offsite to fulfill your duties.

No Other Reasonable Means - There is no alternative to taking the record offsite.

Securing Confidential Hard Copy and Electronic Records

A basic security expectation is that confidential records in hard copy be kept in a "secure institutional environment." Confidential electronic records must be kept and accessed in a secure server environment whenever possible. This means that they reside on a secure server, are accessed from your computer at the University through a recognized departmental or University network or, if working from home, confidential electronic records are accessed remotely using encrypted secure means such as virtual private network or encrypted remote desktop application.

Secure Institutional Environment

A secure institutional environment is a University office or other building location where:

1. The public is not given access,
2. Access is limited to authorized individuals with a need-to-know,
3. The location can be securely locked, and
4. Records are kept in a locked cabinet, drawer or other secure storage area.

Secure Server Environment

The following checklist sets out key factors for IT staff to consider in determining whether a computer may be considered a "secure server". Due to the wide variety of existing and future server operating systems and hardware, specific security procedures and guidelines will necessarily be much more detailed. However, a "no" answer to any of the following questions may point to serious security vulnerabilities for servers intended to store confidential information. Please consult with the department or individuals responsible for administration of your system as they will be best able to assess the security of your server environment.

1. Is the server dedicated to the storage of non-public information?
2. Is the server administrated by a full-time information technology professional?
3. Are all account management and login activities logged, and regularly reviewed?
4. Are individually-named accounts, with strong passwords, created for each user?
5. Has the operating system's default "guest" account been deactivated?
6. Is the "administrator / root" account used only for actual system administration?
7. Are operating system patches installed on a regular (ideally automatic) basis?
8. Is anti-virus software installed, and set to automatically update?
9. Is a firewall, or similar packet filtering software, in use?
10. Is the server located in a physically secure, limited-access location?
11. Is there cooling available to keep the server within its rated heat specifications?
12. Is an uninterruptible power supply (UPS) in use to protect from power problems?
13. Have all unneeded services and ports been stopped?
14. Has a vulnerability scan been run on this server, and deficiencies addressed?
15. Is encryption required when connecting from an external network?
16. Is the server backed up regularly, with restore capabilities tested periodically?
17. Are the backup tapes/media stored in a separate, secure physical location?
18. Is a procedure in place to securely delete data from the server and all backups?

<u>Security Considerations When Taking Hard Copy Records Outside Secure Environments:</u>

If possible, take copies, not originals. Take as few records as you can for expected work, e.g. if you teach a class of 300 students and expect to grade 15 to 20 of their papers over a weekend, take about 20 home to reduce risk.

Carry records in a locked satchel or case. Do not leave records unattended, e.g. at restaurants, washrooms, public transit, etc. Don't read where others could see records.

Protect records from unauthorized individuals, including family or friends. Lock records away when not in use, e.g. in a locked cabinet in your locked home.

Carefully avoid other inappropriate disclosures including:

- Casual disclosures to family, friends, co-workers
- Discussion of confidential information in public areas, like hallways or coffee line-ups
- Unauthorized people overhearing your cell phone conversations

Security Considerations When Taking Electronic Records Outside Secure Environments:

Access records remotely only on authorized, secure networks with encrypted communication.

Use a strong password to protect your electronic devices and laptop, e.g. 10 or more characters long, no dictionary words, at least one capital letter and one number/symbol.

Ensure your computer security is up-to-date, including firewall, anti-virus and anti-spam.

Electronic records taken out of a secure University IT environment should be fully encrypted using an industry standard algorithm at all times.

Seek your department's IT staff for advice on encrypted technology solutions appropriate for protecting electronic data offsite. For the University's Information and Technology Services Department's encryption solutions and for other security resources see:

www.utoronto.ca/security/UTORprotect/

University of Toronto Encryption resources:
http://www.utoronto.ca/security/UTORprotect/encryption_guidelines.htm

Adobe Encryption of PDF documents:
http://help.adobe.com/en_US/Acrobat/9.0/Standard/WSD012A4E1-51D1-4bcd-BA9F-EF03C6F20BB6.html

Encrypting Windows XP records - http://support.microsoft.com/kb/307877

Clean Desk

Purpose and Objective

This practice is about protecting personal or confidential information from unauthorized access by putting it away (clean desk) if you are absent for any substantial period of time.

Checklist

☐ 1. Know which records contain personal or confidential information.

☐ 2. Keep personal/confidential information securely locked when it is not in use or if you are not present to prevent unauthorized access.

☐ 3. Set your computer or mobile device to deny access without a password after you are absent for a few minutes. (5-10 minutes recommended).

Background

Personal and confidential information should be secured or locked away if you are absent. Remove it from your in-tray, work station and printer/copier/fax machine.

Password protect all IT resources, encrypting all that are not secure institutional servers. Set them to lock after 5 or 10 minutes absence or inactivity.

When securing personal or confidential information, consider all foreseeable exposures including, e.g. after-hours cleaning/maintenance visits to your office, emergencies and co-workers without a need-to-know.

Secure Destruction

Purpose and Objective

Secure destruction of personal and confidential information renders it irretrievable to avoid unintended or unauthorized access after disposal of records.

Checklist

☐ 1. Know which records contain personal or confidential information.

☐ 2. Know when records require secure destruction under retention schedules.

☐ 3. Destroy records promptly – do not store records for later destruction.

☐ 4. Know which methods are effective for destroying the media/records in question.

☐ 5. Match destruction methods to the sensitivity of the information being destroyed.

Background

Destruction should be secure. This means using methods, personnel and facilities that ensure information will be destroyed without being copied, used or disclosed before or instead of being destroyed. Match destruction methods to the information sensitivity.

Destroy records immediately. Never accumulate sensitive records for later destruction as this creates security risk which contributes to privacy and confidentiality vulnerabilities.

Destruction renders information irretrievable, by erasing or destroying the medium on which it resides and thus the information. For magnetic media, contact the University's Information and Technology Services department which has a degausser for the purpose.

Ask your department's IT staff for assistance in erasing computer hard drives. Simple erasure does not destroy drive data. Numerous successive overwrites are necessary.

www.dban.org provides a free disk that securely deletes the contents of a hard drive.

Destroy storage media such as compact disks by shredding or cutting into small pieces. Information from "destroyed" media can sometimes be recovered through sophisticated forensic methods, e.g. total destruction of CD/DVD data requires physical scraping off the disk's aluminum layer.

Destroy paper records by crosscut shredding them, either within your office or by a professional destruction company which periodically picks records from a locked shredding bin.

Never discard confidential or personal hard copy records in a recycling or garbage bin.

Records must be securely handled during disposal. Fully document all process steps until destruction so you can later verify that secure destruction occurred without any unauthorized copying or disclosure of the information.

You may wish to consult the Information and Privacy Commissioner's Secure Destruction of Personal Information Fact Sheet at:

http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf

Privacy Event Response

Purpose and Objective

Privacy issues should be immediately reported to management and the FIPP Office to enable timely notification of affected individuals, prompt remediation and reporting. This practice sets a very low threshold for reporting privacy matters to ensure that they come to the immediate attention of individuals and offices who must address them.

Checklist

☐ 1. Immediately report any mishandling of personal information to your supervisor, Divisional FOIL and/or the FIPP Office. Don't delay. Err on the side of over-reporting. If uncertain, ask your supervisor, FOIL or the FIPP Office.

☐ 2. Fully assist your manager, FOIL and/or FIPP Office, as required, to promptly:

- ☐ a. Assess the scope of the breach - who had unauthorized access to personal information, which information was involved, how many individuals affected etc.
- ☐ b. Immediately contain the breach, e.g. retrieve records, confirm destruction, suspend the activity, take the application off-line, change passwords etc.
- ☐ c. Notify affected individuals – including a description of what happened with sincere regrets, an explanation of corrective steps taken and how the problem will be prevented in the future.
- ☐ d. Investigate - identify causes/circumstances around the breach including whether it was inadvertent. Review policies, procedures and security measures.
- ☐ e. Prevent future breaches - Take steps such as developing or changing policy or practices and providing staff training on privacy and security.

Background

Privacy is breached when personal information is collected, retained, used or disclosed inconsistent with FIPPA rules. A common breach is loss, theft or accidental disclosure of personal information, e.g. emailing to wrong parties, lost or stolen unencrypted computers or memory sticks, break-in to your office, home or vehicle.

The University is responsible for the proper handling of personal information. It is essential that privacy breaches be identified quickly, so effective remediation can be aggressively implemented as soon as possible.

Records Management

Purpose and Objective

This practice supports record creation in support of University functions, focusing on records retention schedules; defined accountability; and minimizing risks.

Good management supports record identification and tracking and version control, while preventing duplication, loss, unnecessary searching and creation of unnecessary records.

Checklist

☐ 1. Establish and communicate which office/individual is responsible for creation, maintenance and disposal of records in your unit.

☐ 2. Only create records needed for business purposes or to demonstrate due diligence.

☐ 3. Record all necessary information, but nothing irrelevant or inappropriate.

☐ 4. Know who is authorized to access records with which you work.

☐ 5. Keep University records according to records retention schedules applicable to your operational area and discard insignificant transitory records on an on-going basis.

Background

Records management practices should: align with and support business functions and requirements; support operational efficiency; be cost-effective; be simple for staff to implement; and apply to entire record life cycles from creation to disposal.

Because FIPPA defines “record” broadly, as “any record of information however recorded”, all recorded information at the University falls under this practice. This includes hard copy, electronic, e-mail, audio/video records etc. on any recording or storage medium or system.

Records are needed for the University to: carry out its functions; achieve its goals; make informed decisions and demonstrate due diligence and accountability. It is important to quickly find records needed for business purposes.

Official records, such as decisions, practices, policies, legal papers, audits and public documents should meet the highest possible quality standards. You should also create quality professional records in your everyday work, including rough notes, drafts and routine matters. Although these “transitory” records are not intended to be permanent, while they exist, they are potentially releasable pursuant to legal obligations, such as access requests. Therefore, always create quality, professional records, including emails.

Only create records as needed to support work objectives. The following general parameters can help you to assess your documentation requirements.

1. Know which activities are your unit's and your position's responsibility.
2. Decide what to record; is it required by law or policy or operationally necessary?
3. Decide if a record is needed. Sometimes a telephone call can replace an email.
4. Do not record personal views, inappropriate comments or unnecessary information.

Identify and assign an office or individual to be responsible for each record category and type. That person/office will create, use, store or dispose of the record in question.

Follow records retention schedules to know how long and how to keep records, as well as their disposition, i.e. destroy or transfer to University Archives. See the University File Plan at the website below. If no records schedule exists for your unit, obtain approval from the University Archivist before disposing of records. Information on records management best practices can be found at the Archives' web site: http://utarms.library.utoronto.ca/university-administrators

Metadata is information, associated with a record, which describes the record and its context. Metadata helps to track a record and its various versions, through its lifecycle, by describing record attributes such as ownership, version, history and type.

Metadata can help staff with quick retrieval and to understand whether a record is the final, approved, or latest version, or to know the time of creation/revision of the version. Metadata helps an individual reviewing a record to know which office and official is responsible for the record and the current status of that record and version. The usefulness of metadata depends on the fields chosen and on an operational area's commitment to consistent and full implementation of metadata across record holdings.

Some commonly used metadata fields include:
1. Originating office/author/owner
2. File plan classification
3. Recorded information management requirements (including retention)
4. Document purpose:
    a. Official for public communication
    b. Final, approved
    c. For information
    d. For comment
    e. For input/revision
5. User rights; is document read only/shareable/printable?
6. Security/privacy/confidentiality of information:
    a. Does document contain personal/confidential information?
    b. Circulation/access characteristics of document, i.e. need-to-know, defined group, general internal circulation, public.
7. Version number (e.g. Unit Action Plan v2)
8. Date and time of initial creation/or current version (e.g. 2010-07-24 1:35 PM)
9. Filename and path

Consult metadata to ensure records are only used for intended purposes and are destroyed when required by record retention schedules.

Recording Meetings

Purpose and Objective

This practice supports recording of meetings to support their purpose(s), with appropriate protection of confidentiality.

Checklist

☐ 1. Clearly understand meeting objectives. List them if necessary.

☐ 2. Establish what information must be recorded to support the meeting objectives.

☐ 3. Establish exactly what will be recorded (format, content and level of detail).

☐ 4. Establish who will officially record the meeting.

☐ 5. Ensure other participants do not create “alternative” meeting records.

☐ 6. Establish timing and procedures for finalizing and circulating the official record.

☐ 7. Establish parameters to protect confidential information discussed at the meeting.

Background

Meeting recording practices should align with defined meeting objectives and follow University record management practices.

The purpose of a meeting is to create a result or a set of results. Only create and keep records that reflect the purpose and results of the meeting.

Decide what records need to be created based on:

1. The purpose and objectives of the meeting,
2. Specific operational requirements related to meeting business,
3. University record keeping requirements,
4. Policy and law,
5. Other applicable requirements.

Clearly delineate what the record will contain and not contain, i.e. which facts/information need to be documented to support the business of the meeting?

Designate an individual(s) responsible for creating/maintaining/distributing the record. Responsibilities of this individual(s) include how will the record be created, maintained, used, disclosed, and made available, e.g.:

a. Intended access - public, restricted, need-to-know etc.
b. Timing of production and availability
c. Process for dissemination

Determine in advance how notes and other information, not included in the official record, will be treated. Inform attendees of meeting recording requirements. Instruct attendees respecting their notes/collateral meeting records.

Decide in advance how personal/confidential information will be shared, discussed and/or recorded at the meeting. Consider all relevant factors including:

1. Do all meeting attendees have a need-to-know personal/confidential information?

2. Ask attendees to follow privacy/confidentiality requirements for meeting information.

3. Ensure records contain only information that can be disclosed to meeting participants.

The format, content, level of detail and scope of the records should be only what is necessary to meet the meeting's objectives.

Prevent the creation of unofficial, "alternative" meeting records. Parallel records can be inaccurate, incomplete, or inconsistent with official meeting records.

University meeting records can be requested – and many disclosed under FIPPA. Clearly defining the official meeting record and practices around parallel records will address concerns around possible public disclosure.

Privacy Tips

Purpose and Objective

These tips are intended to help you meet privacy requirements. They are not a full listing of all legal or practice requirements. Detailed privacy guidance is set out in the practices, such as collection, use, disclosure and secure destruction. Contact your Divisional Freedom of Information Liaison (FOIL) or the FIPP Office for specific guidance.

Tips

1. Collect, use and disclose personal information only as necessary for official, established University functions.

2. Only share personal information with the individual to whom it pertains and with officers, employees, agents or contractors who need it for University business.

3. If you have any doubt about disclosing personal information, check with your manager, FOIL or the FIPP Office or obtain consent from the individual.

4. Avoid emailing or faxing personal information or leaving confidential information on a voice mail message.

5. Avoid writing unnecessary personal comments in your communications.

6. Retain personal information for at least one year after the date of its last use.

7. Use effective security such as clean desk, locked cabinets, passwords and encryption.

8. Prevent loss, theft or exposure – e.g. do not leave personal information in a vehicle.

9. Protect privacy in all contexts, including meetings, work and social conversations.

10. Do not leave documents on a fax machine, photocopier, or printer.

11. Build privacy protection into contracts with third party service providers.

12. Report possible privacy issues to your supervisor immediately.

13. Dispose of personal information securely, e.g. cross shred. Do not discard in a recycling or garbage bin.

14. Conduct a privacy impact assessment to ensure proposed new technologies, information systems etc. meet privacy requirements (consult with FIPP Office).

15. When dealing with personal information, err on the side of protecting privacy.

Access/Records Management Tips

Purpose and Objective

These access/records management tips are intended to ensure that access and records management requirements are met. They are not a full listing of all legal or practice requirements. Detailed access/records management information is set out in the practices, such as those for records management and recording meetings. Contact your Divisional Freedom of Information Liaison (FOIL) or the FIPP Office for specific guidance.

Tips

1. Access legislation generally covers all records, including drafts and e-mails.

2. When creating records, always keep in mind the possibility of later disclosure.

3. Only create the right records that are needed for –and defined by– business purposes.

4. Be thoughtful when creating records: Include all necessary information, but never irrelevant or inappropriate comments.

5. Follow office and University records management and retention standards.

6. Clearly designate responsibility for records to avoid duplication and confusion.

7. Ensure that you do the following for records over which you have responsibility:
    a. Store securely,
    b. File records for convenient access and quick retrieval,
    c. Know the record's status – draft, final, official version for circulation, etc.,
    d. Know who is/are authorized to access the record,
    e. Dispose of transitory records; unnecessary/superseded copies/versions promptly.

Other Resources

Privacy and record keeping are generally common sense. Official University activities are based on sound, established practices.

For questions or concerns, refer to the relevant practice(s) and consult your manager, Divisional Freedom of Information Liaison (FOIL) and/or the FIPP Office.

University of Toronto Freedom of Information and Protection of Privacy Office:

Website:
http://www.fippa.utoronto.ca

Director:
Rafael Eskenazi
416-946-5835
rafael.eskenazi@utoronto.ca

Coordinator:
Howard Jones
416-946-7303
howard.jones@utoronto.ca

U of T encryption information:
http://encrypt.utoronto.ca/home

The Canadian Standards Association (CSA) *Model Code for the Protection of Personal Information* (Q830) contains ten principles for working in a privacy protective manner. The main CSA Privacy Code page can be found at:
http://www.csa.ca/cm/ca/en/privacy-code

The Principles are set in brief at: http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/principles-in-summary

1. Accountability
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. Identifying Purposes
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. Consent
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure, and Retention
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6. Accuracy
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. Openness
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Individual Access
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The Information and Privacy Commissioner/Ontario has developed Privacy by Design (PBD) for development and delivery of activities which involve personal information;

1. Proactive not Reactive; Preventative not Remedial - The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize – it aims to *prevent* them from occurring.

2. Privacy as the Default - PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required by the individual to protect their privacy – it is built into the system.

3. Privacy Embedded into Design - PbD is embedded into the design and architecture of IT systems and business practices. It is not an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality; Positive-Sum, not Zero-Sum - PbD seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretence of false dichotomies, such as privacy *vs*. security, demonstrating that it *is* possible to have both.

5. End-to-End Lifecycle Protection - PbD, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, PbD, ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency – PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy – PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Information about Privacy by Design can be found on the Information and Privacy Commissioner/Ontario PbD Website: http://www.privacybydesign.ca/