Lunch & Learn – Privacy Protection

19 April 2018
Agenda

- Waterloo Privacy Office
- Privacy Framework
- General Tips
- Sharing Information
- Privacy Breaches
- Safeguards
- Who can Help
Waterloo Privacy Office
- Provides leadership, guidance, and advice
- Develops and facilitates implementation of policies & procedures
- Responds to:
  - access requests
  - privacy breaches
  - complaints
Privacy Framework
Lunch and Learn

Law

Policy

Guidelines
FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY (FIPPA)
Since 2006, all Ontario universities have been covered by FIPPA.

FIPPA requires that the University:
- Provides right of **access** to university information (subject to exceptions); and
- **Protect** personal information held by the University, where applicable.

FIPPA is enforced by the Information & Privacy Commissioner of Ontario (IPC).
Key principles:

- Collect only information you need
- Use only for purpose for which it was collected
- Keep information only as long as necessary
- Access/disclose information appropriately
- Dispose of information securely
Use and disclosure:

- When the person has consented
- Consistent purpose
- To an employee who needs it to perform their duties
- Safety of an individual
Personal information

- Name, address, home and cell number
- Education, financial, medical history
- Race, religion, age, marital status
- ID number
- Written comments and opinions about a person (whether student, faculty, staff or other)
- the personal opinions or views of the individual except where they relate to another individual
POLICY 46
INFORMATION MANAGEMENT
- Provides security classification scheme for university information
- Outlines responsibilities members of university community have with respect to information security
- Defines student information
- Sets the rules re: need for security controls and breach/loss response
- Restricts access only to Waterloo instructional or administrative staff with a legitimate need
- Very little student information is considered public
Student Information

- Name
- Phone number
- Student number
- Email
- Grades
- Class lists
- Student assignments
- Discipline records
Public Student Information

- faculty or college of enrolment
- programs of study
- sessions in which a student is or has been registered
- awards based on academic merit
- degrees received and dates of convocation
GUIDELINES FOR MANAGING
STUDENT INFORMATION

GUIDELINES FOR SECURE
DATA TRANSMISSION
GENERAL TIPS
- Collect/record only the information you need
- Be objective and factual
- Assume access (includes emails)
- Handle confidential records confidentially
- Dispose of transitory records
- Use secure disposal methods
E-mail messages are records

Email containing sensitive personal or confidential information

- Verify the e-mail address of recipients
- Avoid using “reply to all” feature
- Avoid email lengthy chains
- Ensure correct attachments!!
- Return to sender notification
- E-mail messages that could be released in an access to information request
  - Email between faculty about a student
  - Email from someone else about a student
  - Emails between instructors and TA’s
Sharing Information
- Need to know?
- Would the student see disclosure as reasonable?
- What about mom and dad?
- Getting consent to share
Privacy Breaches
What is a Privacy Breach?:

- Loss
- Unauthorized access
- Unauthorized disclosure
- Unintentional or intentional
<table>
<thead>
<tr>
<th></th>
<th>Loss</th>
<th>Access</th>
<th>Disclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unintentional</strong></td>
<td>Misplaced file</td>
<td>Mistakenly look at a file not related to your work</td>
<td>Show file to wrong student</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mistakenly send email to wrong student</td>
</tr>
<tr>
<td><strong>Intentional</strong></td>
<td>Shred file</td>
<td>Look up marks of your neighbor’s child</td>
<td>Tell your neighbor what you saw</td>
</tr>
<tr>
<td></td>
<td>Destroy file</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stolen file</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Responding to a Privacy Breach

1. Contain
2. Notify
3. Investigate & Remediate
Responding to a Privacy Breach

- Retrieve hard copies
- Ensure no copies have been made
Responding to a Privacy Breach

- Notify the individuals & Provide details of breach
- Notify IPC (?)
Responding to a Privacy Breach

investigate & remediate

Lunch and Learn
1. Review circumstances of breach
2. Review adequacy of polices & procedures
3. Identify ways to prevent future breaches
4. Implement recommendations (education, training, new procedures)
5. Share findings of investigation

Lunch and Learn
Safeguards
Physical
• Locked drawers, cabinets, doors
• “clean desk”, shredder

Administrative
• Legislation, policy, procedures
• Good business practices (verify IDs)
• Training

Technical
• Secure passwords, VPN, updates, anti-virus
• Encryption, encrypted portable devices
Department/ Faculty

- ??

University Resources

- Privacy Officer: Kathy Winter ext 36101
- Privacy Administrator: Melissa Holst ext 36125
- University Records Manager: Chris Halonen ext. 38284
- Information Security Services: Jason Testart

Province

- Information and Privacy Commissioner of Ontario
  1-800-387-0073
Questions?