Privacy and Flexible Work Arrangements

University of Windsor

April 2022

Legal Services

Table of Contents

Welcome to the University of Windsor's Privacy and Flexible Work Arrangement Training Program.

The protection of University of Windsor data is becoming an increasingly important and difficult task. This has been especially true through the COVID-19 pandemic. As technological advancements are developed, and with an increased reliance on home offices and flexible work arrangements, it becomes more and more difficult for all entities large and small to protect the confidential data that they possess. Our hope is that after this training module University of Windsor employees will be better prepared to address these challenges, and to provide the University of Windsor Community with confidence that the University and its employees are taking the necessary steps to protect their privacy.

Privacy and Confidentiality

- Employees must protect all Confidential Information
- "Privacy" obligations are only relevant in relation to Personal Information that is in the custody or control of the University

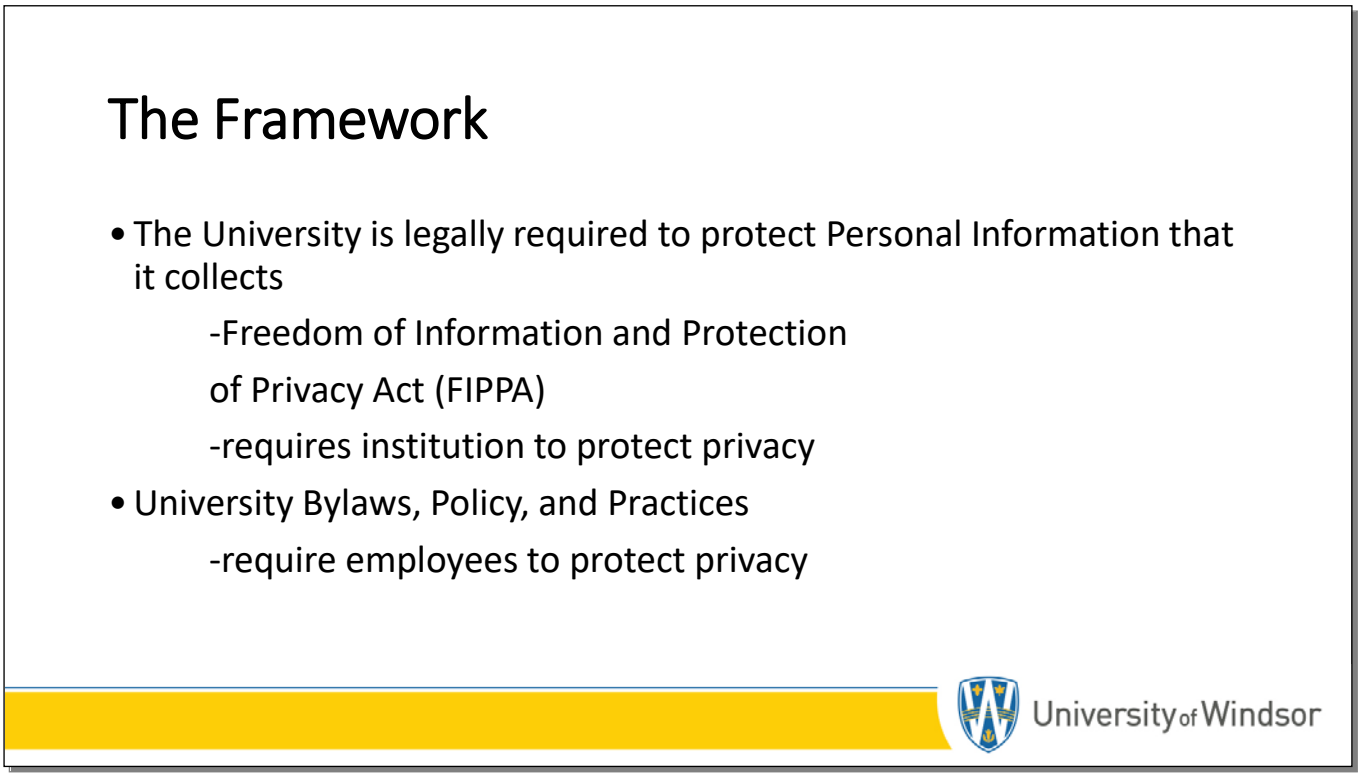
University of Windsor

All university employees share in the responsibility to protect university confidential information. The University does not have a formal definition of what constitutes confidential information, however, in general terms, confidential information is information that is not available publicly.

Privacy on the other hand is a slightly different concept. All data that is subject to Ontario privacy laws will be confidential, but not all confidential information will be subject to Ontario privacy laws. When we talk about privacy, it is important to understand this important distinction.

Privacy concerns itself with the protection of "Personal Information", and this training program will focus on the protection of personal information that is in the custody and control of the University and the steps that university employees can and should take to identify and protect the Personal Information of the people who live, work, study, at the University of Windsor.

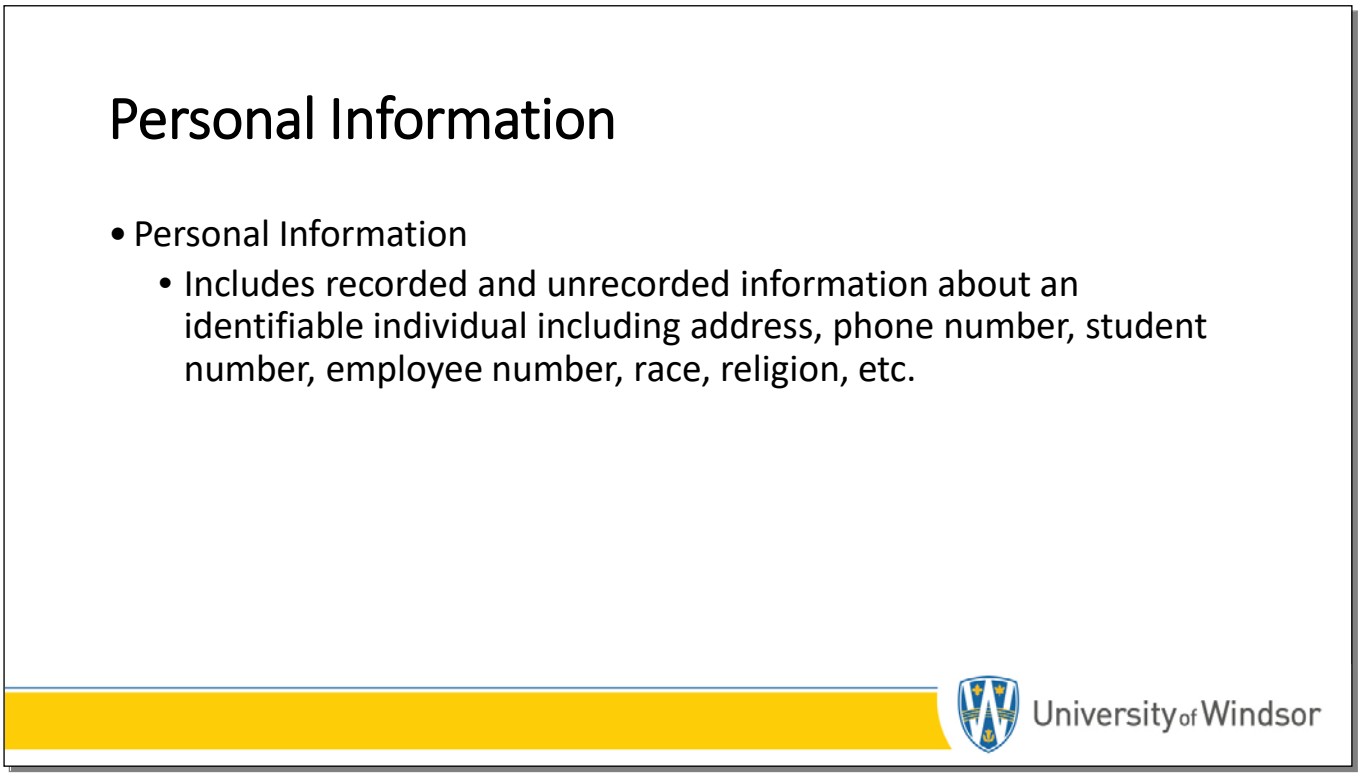
This module will shortly go into more detail about Personal Information.



The framework that guides the University of Windsor's privacy efforts is as follows:

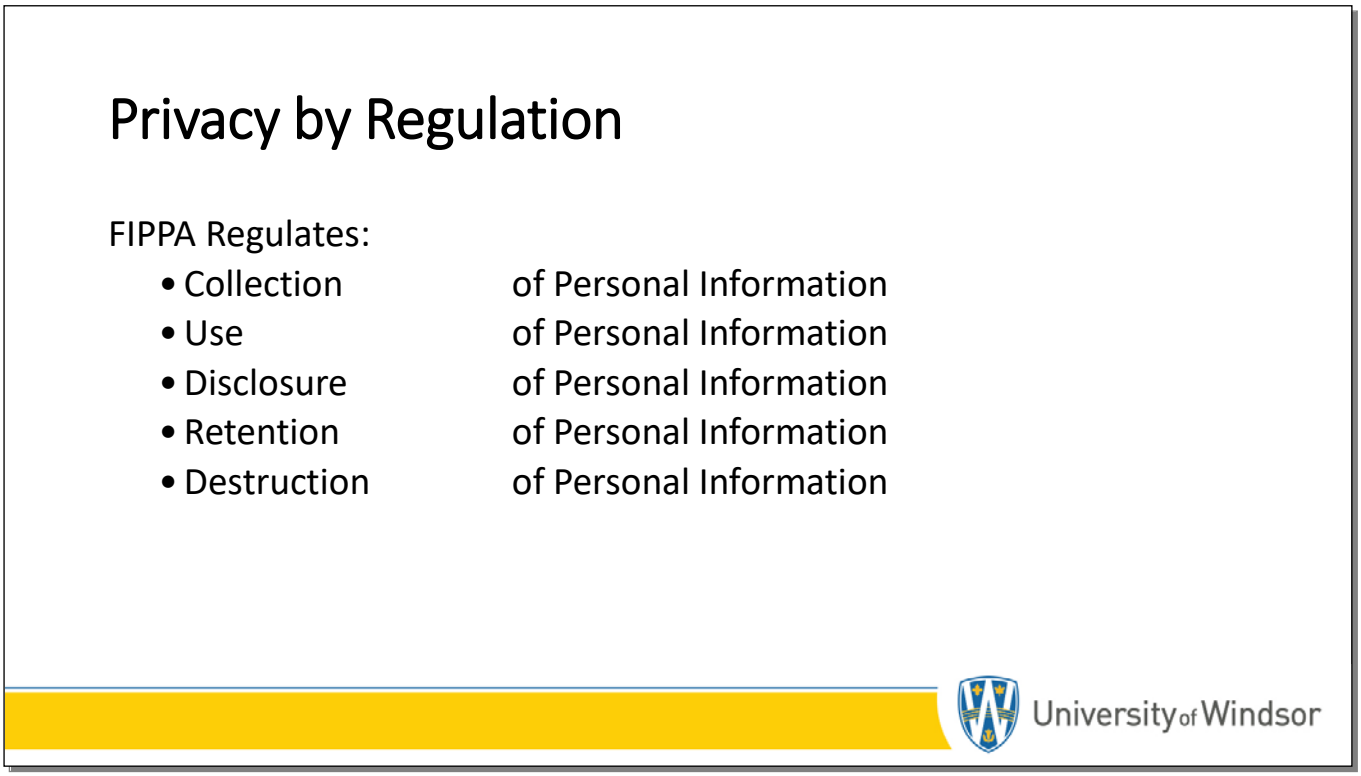
1. Firstly, there is the Freedom of Information and Protection of Privacy Act ("FIPPA"), for short. The University of Windsor has been subject to FIPPA since June 2006. FIPPA is the privacy legislation that regulates the Provincial Government and Provincial agencies in their collection, use, disclosure, of personal information. In June 2006 Ontario University's were brought under the jurisdiction of FIPPA and have been operating under it ever since.

2. Secondly, there are the University's bylaws, policies, and practices in relation to privacy and/or the protection of personal information. The University has numerous bylaws, policies and practices that touch upon the protection of personal information. It will be important to familiarize yourself with these. You can feel free to discuss with your supervisor and/or the Department of Legal Services which bylaws, policies and practices may impact your respective areas.



A key concept in the discussion of privacy is the definition of "Personal information". Section 2 of FIPPA provides us with a definition of Personal Information that includes a list of examples as to what qualifies or doesn't qualify as Personal Information, but generally speaking Personal Information includes recorded and unrecorded information about an identifiable individual and including such things as address, phone numbers, student numbers, employee numbers, date of birth, race, religion, and other personally identifying data points, etc.

In short, the definition of Personal Information includes things that most people would identify as being personal in nature. It is also important to note that in the privacy context, personal information does include unrecorded information and that privacy laws protect recorded and unrecorded information. It is important to note that the unauthorized disclosure of a document that contains personal information may be a privacy breach, in addition, any verbal disclosure of personal information may also constitute a privacy breach.



The Act requires the University to protect an individual's Personal Information by regulating the University's handling of Personal Information. Personal Information is regulated in five ways. The Act regulates the University's collection, use, disclosure, retention, and lastly destruction of personal information.

Collection:
The University is required to provide notice to individuals from whom they collect personal information. That notice must contain

- the authority under which the University is collection the information
- the purposes for the collection or the intended use of that personal information and
- the name of a contact information of a person they can be contacted about questions in relation to the collection.

Use:
The University may use personal information that it has collected for the purposes outlined in the University's notice of collection and where it has obtained the consent of the individual to whom the information relates. Personal Information may also be used by the University for any other purpose permitted by the Act.

Disclosure:
The University may disclose personal information where that disclosure is provided for the University's notice of collection. The University may disclose personal information to an officer

or employee of the University, if the officer or employee requires the information in the performance of their duties, and the duties are necessary and proper in the discharge of the University's function. The University may also disclose Personal Information for any other purpose permitted by the Act.

Employees with questions or concerns about the disclosure of personal information should contact their supervisor or Department Heads.

Retention:
Once Personal Information has been collected by the University, it is required to retain that personal information for a period of one year beyond its collection or its last use. The University may destroy Personal information outside of the one-year rule if it obtains the consent of the person to whom it relates.

Destruction:
The destruction of personal information whether contained on paper records or stored on computing devices, must be done with care. Paper records must never be thrown in the garbage or recycling. Paper records containing personal information should be destroyed by cross-cut shredding in university provided shredding bins.

For electronic files simply deleting a file from a storage medium may not be sufficient. The physical destruction of the storage medium may be necessary. Please consult with IT Services to discuss best practices around deleting personal information from computing storage devices.

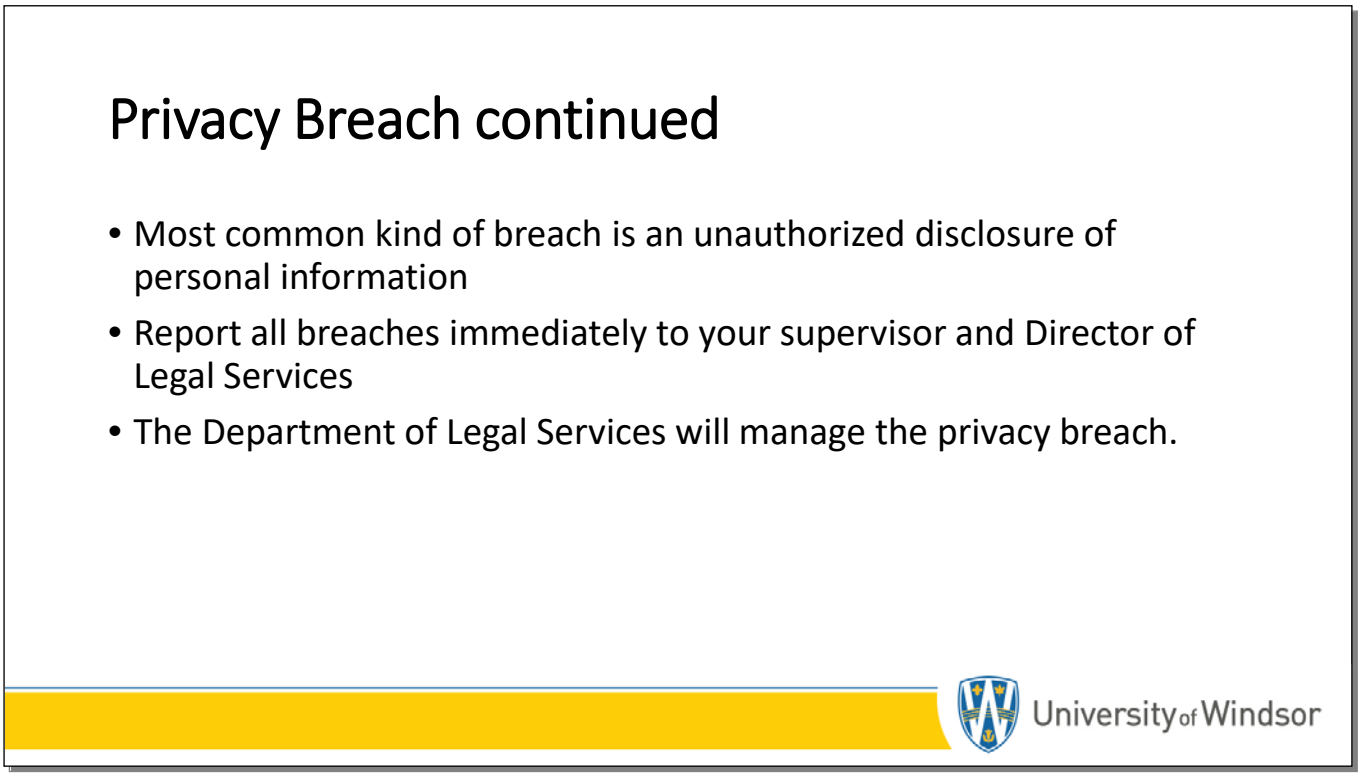
Privacy Breach

- What is it and what to do when it occurs
  - -unauthorized access
  - -improper use or disclosure

- Privacy Breach Protocol
  - -contact Legal Services

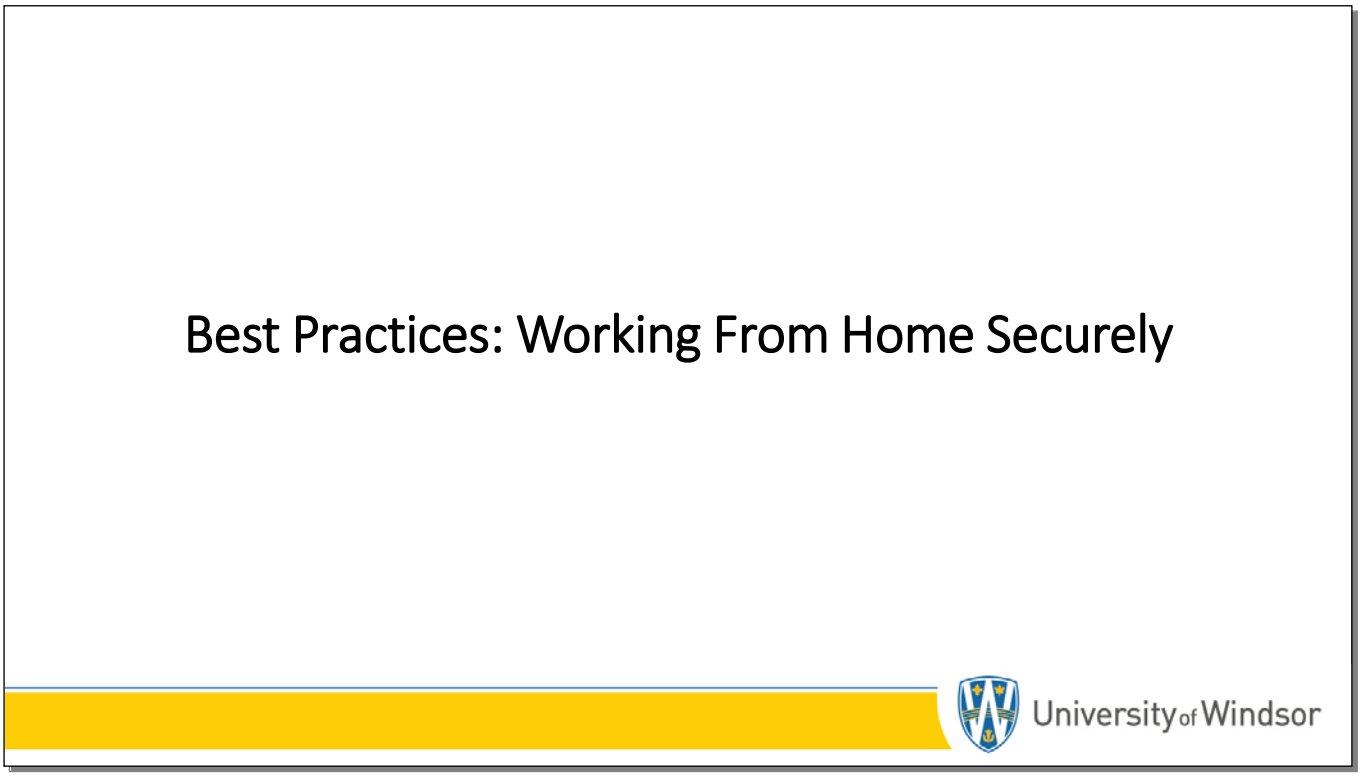
University of Windsor

Now we have spent some time talking about what privacy is, what it applies to and how the University protects privacy, what happens when that process breaks down? This is called a privacy breach. A privacy breach is an institution's failure to collect, use, disclose, retain and/or destroy Personal Information in a way that is consistent with its obligations under FIPPA.



The University and all of its employees work very hard to make sure that Personal Information is safe and secure. However, errors do happen, and privacy breaches do occur. By far the most common type of privacy breach is an unauthorized disclosure of personal information. These breaches are most often a result of email being accidentally sent to the wrong recipient or containing the wrong attachments. If a Privacy Breaches occurs all employees must immediately report the breach to their supervisor and the Department of Legal Services and time is of the essence.

Time is very important when handling a privacy breach. If the University acts quickly enough it can sometimes retrieve email that are accidentally sent to the wrong recipient. While such an instance is still a privacy breach the retrieval of the errant message greatly reduces the risk of harm to the person whose personal information has been disclosed. The University has a Privacy Breach Protocol that helps guide the University response to a privacy breach. The University's privacy breach response will be coordinated by the Department of Legal Services and can be found at [attached Privacy Breach Protocol].



As discussed, the University of Windsor is subject to regulations regarding the privacy and confidentiality of information. As the Flexible Work Arrangement Program is an option for eligible employees, the privacy and confidentiality requirements must continue to be met by all remote working employees. Remote workers are required to take all reasonable steps to secure and maintain the privacy and confidentiality of University of Windsor information and records. Remote working has associated risks and the following sections of this module will outline some best practices for limiting your exposure to those risks.

Suggestions for working from home securely:

- Personal Information used in connection with your work should only be kept on encrypted University owned devices. If you are not sure about a device contact IT Services. Assistance can be provided for any University owned devices

To start, Personal Information used in connection with your work should only be kept on encrypted University owned devices. These devices may include cell phones, tablets, or personal computers. Encryption protects against a data breach even if the device is lost or stolen.

If you are not sure whether your university owned device is encrypted, please contact IT Services.

Continued

- Use strong passwords for home Wi-Fi networks
- Use University provided computer resources where possible.
- Do not permit family members or others to use University provided equipment
- Avoid where possible mixing workspaces in the home with personal/family spaces
- Use a VPN to connect to the campus network
- If you know of or suspect that you have a security problem, contact IT Services and/or Department of Legal Services

University of Windsor

When working from home, secure your home network by using strong passwords, usually 12 characters, for your home Wi-Fi networks. Ensure that your home internet router has all the vendor software patches installed. If you rent your router this may be done automatically by your internet provider. Or, if you own your router, you will need to verify this yourself through the router's manufacturer.

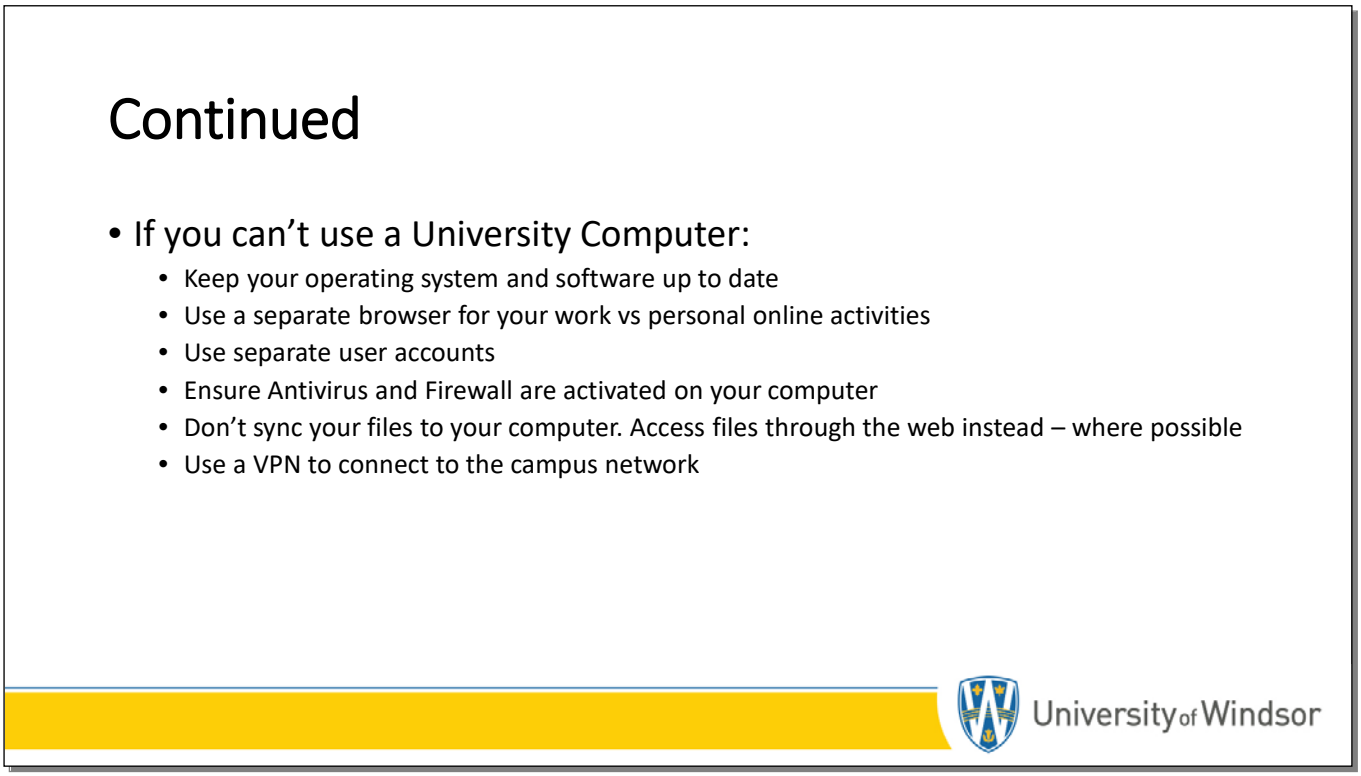
Use University provided computer resources where possible.

Do not permit family members or others to use University provided equipment. In addition to being encrypted, devices must be password protected and those passwords must not be shared with others, including family members.

Avoid mixing workspaces in the home with personal or family spaces. This includes taking all reasonable steps to ensure your screen content is not viewable and phone and video conversations involving personal or confidential information cannot be overheard by others in the home, and secure work-issued and personal computing devices when not in use or when left unattended.

Use a VPN to connect to the campus network. A VPN encrypts all traffic between your computing device and the University's firewall. It protects against eavesdropping by hackers and ensures you have access to the resources you need.

Contact IT Services or the Department of Legal Services if you know of or suspect a security problem.



If you can't use a university issued computer or device:

- Keep your operating system and software up to date.
- Use a separate internet browser for university work and personal online activities
- Use separate user accounts on your devices. Most computer operating systems allow for multiple user accounts to be made.
- Activate antivirus and firewall on your computer and ensure the anti-virus is regularly updated.
- Don't sync your files to your computer. Access files through the web instead, where possible. Instead, use Microsoft 365 and OneDrive to save and sync your files.
- Use a VPN to connect to the campus network, as previously mentioned.

Continued

- Hardcopy records must also be kept confidential and secured (locked if possible)
- Disposal of record containing Personal Information need to be destroyed by crosscut shredding. Do not place in garbage or recycling.
- Exercise caution when travelling with confidential and/or private information.

University of Windsor

Working remotely is not limited to using electronic documents and communications. There may be a scenario where hardcopy records and files are used. With respect to hardcopy records, employees must ensure those records are kept confidential and secure from all unauthorized individuals, including family and friends. To keep these records secure, put the records away when not in use, and if possible, in a locked cabinet, in your locked home.

If records need to be disposed of according to applicable records retention policies, records containing Personal Information need to be shredded using a cross-cut shredder. If a shredder is not available to you at your flexible work arrangement location, bring the records to the University for appropriate disposal. Do NOT under any circumstances dispose of records in recycling or garbage bins for regular municipal pick-up.

Exercise caution when transporting records containing personal or confidential information. Carry records in a locked bag or case if possible and never leave the records unattended – in a car, restaurant, or on public transit, etc. Move the records directly from home to the university office.

University Resources

Department of Legal Services

- http://www.uwindsor.ca/legal-services/

FIPPA

- https://www.uwindsor.ca/legal-services/298/freedom-information-and-protection-act

IT Services

- http://www.uwindsor.ca/itservices/1064/working-home-campus

University of Windsor

You will find some helpful resources on the Legal Services, FIPPA, and IT Services webpages. Please do check back often as we continue to make resources available.

Contacts

- **Richard Taylor**, Director of Legal Services
  Ext# 4059 richard.taylor@uwindsor.ca
- **Julie Laforet**, Insurance, Risk and FIPPA Officer
  Ext# 2080 jlaforet@uwindsor.ca
- **Ericka Greenham**, Manager of Client Services, IT Services
  Ext# 5375 ericka.greenham@uwindsor.ca

University of Windsor

This concludes this module on privacy for flexible work arrangements. Feel free to reach out the Department of Legal Services and/or IT Services who can provide additional assistance with any questions or concerns that you may have about keeping University records that contain Personal Information safe and secure when working from home.