Through positive information security behaviours we can all assist in protecting our valuable research, teaching and administrative resources.

Top 10 “Things to Know”

1. Users should be aware, that the university does not guarantee security - users should always engage in “safe computing” practices.

2. The university shall disclose any breach of the security of an information system to any individual whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

3. Any computer or network security incident that potentially involves criminal activity shall be reported to Campus Community Police.

4. Everyone who connects a computer to university computing resources has the potential to affect the security of those resources.

5. Encryption of wireless communications is required for all staff and faculty at the university.

6. All users are responsible for classifying the data that they are using in their environment in accordance with the data classification definitions.

7. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

8. Unit Heads, including Directors, are responsible for ensuring that security policy is implemented within the unit.

9. Individual users of computing resources must be familiar with, understand, and comply with relevant laws, policies, and procedures governing their use of the university’s computing resources.

10. When engaging in electronic communications with persons in other jurisdictions or on other systems or networks, be aware that they may also be subject to the laws of those other jurisdictions and the rules and policies of those other systems and networks.

For more information, visit security.uwo.ca
Protecting the privacy and security of information and electronic resources is a priority at Western. The Computing, Technology & Information Resources Policy outlines our collective responsibilities in safeguarding these critical resources.

Policy highlights:

**CODE OF BEHAVIOUR**
Raise your hand if you’ve read the fine print on every licensing agreement for software you’ve downloaded. We understand – detailed rules and regulations can be overwhelming. However, this Code of Behaviour establishes a set of standard expectations for all members of Western’s campus community around the use of computing resources.

**Do these:**
- ensure that the university’s computing resources are used in an ethical and lawful manner.
- read and ensure you understand the Code of Behaviour as outlined in policy 1.13 (www.uwo.ca/univsec/policies_procedures/general.html) as it applies to all users of the university’s computing resources.

**Don’t do these:**
- intentional use of computing resources for any purpose other than academic, administrative, and/or incidental, non-commercial personal use, will be considered to be unauthorized.
- use unlicensed or unauthorized copies of computer software

**Remember:**
Use of university computing resources are not completely private and there are situations, as outlined in the Code of Behaviour, where the university, in its discretion, may disclose the results of general or individual monitoring to appropriate university personal or law enforcement agencies.

Key Principles of the Policy:

1. Academic Freedom is respected, but not to contravention of the Law
2. Use of University systems and data should be limited to specific and authorized purposes
3. Individual users are responsible for the security and protection of any University data that they may need
4. Individual privacy rights must be respected and protected
5. Incidental personal use of university systems is allowed, within reason
6. University provided Computing devices (including phones) and accounts are owned by Western
7. University supplied email addresses are designed as official for purposes of University communication
8. Protocols for handling University data will be informed by Western’s Data Classification standards
9. Specific provisions in negotiated Collective agreements may take precedence over the policy
10. Breaches of the policy will be arbitrated based on the user group(s) involved in the breach