UNIVERSITY CANADA WEST

PROCEDURE

Procedure Number:	**8008p**
Procedure Title:	**Acceptable Use of Information Technology Resources**
Approved by:	**President**
Approval date:	**August 24, 2020**
Effective date:	**August 24, 2020**
Review date:	**June 30, 2020**
Next review date:	**June 2023**

1. Purpose

1.1. These procedures are designed to support the Acceptable Use of Information Technology Resources Policy.

2. Information Technology Resources

2.1. In this Policy, "**Information Technology Resources**" means equipment, software, networks, facilities and services used to input, store, process, transmit, view, and output information, including, but not limited to, desktop computers, laptop computers, tablets, mobile and other wireless communication devices, servers, telephone and voicemail systems, printers, scanners, fax machines, copiers, internet, intranet, wifi, education technology, email, social media sites, communications applications, licensed software (including third party software and cloud service tools), hardware, electronic storage media such as CDs, USB memory sticks, and portable hard drives, and all related equipment and infrastructure.

3. Rules and Responsibilities

3.1. Users are expected to conduct themselves reasonably and to exercise good judgement in the use of Information Technology Resources.

3.2. Users must ensure that their use of Information Technology Resources complies with the following:

- All applicable laws, legal requirements and ethical standards, including the BC *Personal Information Protection Act* (the "**PIPA**"), Canada's Anti-Spam Legislation, the *Criminal Code*, and the BC *Human Rights Code*;
- All University policies, including but not limited to this Policy and all policies concerning standards of conduct and bullying and harassment; and
- Third party software license agreements and third party intellectual property rights.

3.3. Users who are issued University email accounts are expected to use those accounts for sending and receiving all emails pertaining to their work or studies at the University. University email accounts are to be used only for University business and not for personal purposes, except as described below.

3.4. VP of Operation and IT Services is responsible for authorizing the use of Information Technology Resources, providing appropriate training to users, issuing and recording system passwords, and monitoring the use of Information Technology Resources reasonably, as necessary or as requested.

3.5. Users of the University's Information Technology Resources must comply with all applicable laws and University policies in the course of such use.

3.6. Users are permitted to use only the software installed by the University. No connection to the internet is permitted except via established University procedures.

3.7. No software shall be downloaded or distributed within the University for any reason, without the University's written approval. This includes but is not limited to all screen savers, shareware, utilities, software and operating system updates.

3.8. Where a user ceases to have access to the University's e-mail system, the User's email address will be deleted within a reasonable period following their departure. In such circumstances, any mail sent to that address will not necessarily be forwarded to another address, but may need to be reviewed by the University to ensure a smooth transition of the User's duties and responsibilities.

3.9. If a User becomes aware that Information Technology Resources are being used in a manner inconsistent with the provisions of this Policy, or otherwise in breach of any agreement or the law, they must immediately report the matter to VP of Operation and IT Services.

4. Prohibited Activities

4.1. The following activities by Users are strictly prohibited:

- Creating, transmitting, distributing, forwarding, retrieving, downloading and/or storing any software, communication, document, file or information that:
    - infringes any copyright, trademark, trade secret, or other intellectual property right;
    - is obscene, sexually explicit or pornographic;
    - is libellous, defamatory, hateful, or constitutes a threat or abuse;
    - is or encourages conduct that would constitute a criminal offence or give rise to liability;
    - bullies or harasses the receiver, whether through language, frequency, or size of message(s);
    - is junk mail, spam or chain email;
    - forges or misleads the sender's identity;
    - exposes the University or its employees to unauthorized legal obligations or liability;
    - divulges private and/or confidential information related to the University's business, students and/or employees; or
    - violates any University rules or policies;
- Using a gmail or other personal e-mail account for University business;
- Downloading from the internet unauthorized programs and/or software;

- Viewing or accessing obscene, pornographic or otherwise inappropriate websites;
- Using another person's password;
- Gaining or attempting to gain unauthorized access to any account on any University system; or
- Using Information Technology Resources for illegal or criminal purposes.

4.2. Any use of Information Technology Resources that disrupts or interferes with the operation of the University's business, or the ability of other Users to utilize them for their intended or authorized purpose, is prohibited. Such prohibited activities include, but are not limited to:

- Destroying, altering, overriding, overloading, dismantling, disfiguring or disabling Information Technology Resources;
- Damaging or altering the hardware or physical components of Information Technology Resources;
- Attempting to circumvent security controls on Information Technology Resources;
- Downloading, altering, plagiarizing, improperly appropriating or storing data or programs in breach of software licenses, copyright laws or third party intellectual property rights;
- Knowingly introducing malware including viruses, worms, Trojan horses and spyware to Information Technology Resources;
- Intercepting or examining the contents of messages, files, communications, accounts or programs without appropriate authorization; or
- Engaging in any uses that result in the unauthorized examination, interception, dissemination, destruction, loss, theft or alteration of another User's information.

5. Security

5.1. Users must take appropriate steps to ensure the security of Information Technology Resources by adhering to all applicable security measures, including using and safeguarding all necessary passwords.

5.2. Users are expected to choose secure complex passwords and avoid using passwords that use sequences or common words (such as "12345", "ABCDE", "55555", etc.) or public knowledge items that relate to Users personally (such as a User's name, address, phone number or spouse's name). Passwords used to secure the Information Technology Resources shall not be used by the User for other purposes or on personally held online accounts with third parties. Sharing passwords or using another User's password constitutes a violation of system security and is prohibited.

5.3. Users must ensure that Information Technology Resources are secured when they are not being used, including logging out of devices when they are not in use.

6. Monitoring, Access and Privacy

6.1. The University has a responsibility to ensure that all email, communications, data and information downloaded, viewed, accessed, created or altered using Information Technology Resources complies with the University's policies and agreements, and with applicable laws.

6.2. The University does not engage in ongoing or routine monitoring of Users' use of Information Technology Resources. However, regular monitoring may occur for legitimate reasons, including troubleshooting, monitoring and addressing network security and performance, addressing system maintenance needs, and evaluating and improving the University's systems.

6.3. Information Technology Resources, and all use of or information contained or stored on Information Technology Resources, may also be monitored or accessed by the University for the following purposes:

- To investigate incidents, complaints or allegations where there are reasonable grounds to believe that student or employee misconduct (or any other inappropriate conduct) has occurred or is occurring, including any violation of University policies, agreements and/or applicable laws;
- To ensure that Information Technology Resources are being used in compliance with this Policy, and any applicable laws; and
- For any other purpose permitted or required by the PIPA or any other applicable laws to access and/or monitor the information stored on Information Technology Resources.

6.4. The University does not guarantee privacy in the use of any of Information Technology Resources, even where used for incidental personal use. Users should be aware that the University has access to and may inspect any information or materials stored, transmitted or created using the Information Technology Resources.

7. Personal Use

7.1. University email accounts are to be used only for University business and not for personal purposes.

7.2. Information Technology Resources must not be used for any purpose that is not specifically related to University business, with the exception of incidental personal use as defined below.

7.3. Incidental personal use of Information Technology Resources is permitted, provided that such use meets all the following criteria:

- It is infrequent and of short duration;
- It occurs outside of working or instructional hours;
- It complies with this Policy and all applicable laws;
- It does not cause the University to incur any cost;
- It does not expose the University to any harm, risk, loss or liability; and
- It is not intended for commercial purposes or personal profit.

7.4. While the University does not encourage personal use of Information Technology Resources, the University recognizes that where such use takes place, the Information Technology Resources may contain or store information or records relating to this personal use, e.g. personal emails, documents, voicemails, text messages, records of internet or social media use, etc. ("**Personal Use Records**").

7.5. While the University takes reasonable measures to back up information and protect it from loss and unauthorized access, the University cannot guarantee that Personal Use Records will be retained within Information Technology Resources or remain confidential. Users who utilize Information Technology Resources to create, store or circulate Personal Use Records do so at their own risk.

8. Sensitive Information

8.1. "**Sensitive Information**" includes (a) personal information (as defined in the PIPA) pertaining to students, staff, faculty or other individuals (e.g., student records, educational records, employment files, etc.), and (b) confidential information of or about the University, its business, employees, students, operations, programs or plans that is not generally known, used or available to the public.

8.2. Where approved, the following rules and security protocols apply:

- Employees must have authorization from their Supervisor before accessing Sensitive Information from remote locations.
- Employees may only access and store Sensitive Information on the Information Technology Resources and the University's systems and networks. If an employee must store Sensitive Information on home computers or mobile devices, the employee must ensure that files are encrypted so that they cannot be accessed by third parties if a device is lost or stolen.
- Unless approved by their Supervisor, employees may not use cloud-based services to store, access or transmit Sensitive Information on Information Technology Resources and the University's systems and networks.
- When using online tools, employees must ensure that they are connected to a private and secure wifi network. Public networks are not an appropriate way to transmit or access Sensitive Information.
- Employees must not use personal email accounts for storage, transmission or disclosure of Sensitive Information.

9. Reporting a Security Breach

9.1. Users must contact VP of Operations and IT Services immediately if they become aware of, or are concerned about, an actual or potential security breach involving Information Technology Resources. A failure to report an actual or potential security breach will constitute a serious breach of this Policy.

10. Breach of this Policy

10.1. Users who misuse Information Technology Resources, or who otherwise fail to comply with this Policy, will be subject to:

- for employees, disciplinary action up to and including suspension or termination of employment,
- for students, disciplinary action up to and including suspension or expulsion, and/or
- revocation or suspension of the User's access to any or all Information Technology Resources.

11. Amendments to the Policy

11.1. The University reserves the right to amend or update this Policy from time to time at its sole discretion.