UNIVERSITY CANADA WEST

PROCEDURE

Procedure Number:	**2700p**
Procedure Title:	**Acceptable Use of Information Technology Resources**
Approved by:	**President**
Approval date:	**August 24, 2020**
Effective date:	**August 24, 2020**
Review date:	**April 2024**
Next review date:	**April 2027**

1. Purpose

1.1. This Procedure is designed to support Policy 2700.

2. Definitions

2.1. The definitions in Policy 2700 apply to this Procedure.

3. UCW Email Accounts

3.1. UCW email accounts are to be used only for university business and not for personal purposes, except as described below.

3.2. The Vice President, 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.

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

4. Third-Party Software Programs or Applications

4.1. Users are permitted to use only the Software, cloud-based services Applications installed by UCW on Computer Hardware or otherwise authorized or made available on Information Technology Resources.

4.2. No connection to the internet is permitted except as under Policy 2700.

4.3. Users must not download, distribute, or otherwise use any other Software and Applications without written approval from the Vice President, Operations & IT Services (or delegate). The

approval could be obtained via direct email or a Helpdesk ticket. This includes but is not limited to all screen savers, shareware, utilities, software programs, applications, and operating system updates.

5. Password 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 (e.g. “12345”, “ABCDE”, “55555”) or public knowledge that relates to Users personally (e.g. User’s name, address, phone number or spouse’s name).

5.3. Passwords used to secure Information Technology Resources shall not be used by the User for other purposes or on personally held online accounts with third parties.

5.4. Sharing passwords or using another User’s password is prohibited.

5.5. 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. Reporting a Security Breach

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

6.2. Users must contact UCW’s Privacy and Data Protection Officer immediately pursuant to UCW’s Privacy Policy if they become aware of, or are concerned about, an actual or potential breach of Sensitive Information.

6.3. A failure to report an actual or potential security breach will constitute a breach of this Policy.

7. Related Policies

Policy Number	Policy Title
2700	Acceptable Use of Information Technology Resources
5006	Academic Integrity
6006	Copyright
6751	Information Privacy and Security
8001	Respectful Workplace
8003	Standard of Conduct
9014	Students Rights and Responsibilities