UCW UNIVERSITY CANADA WEST

POLICY

Policy Number:	**2700**
Policy 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. Policy Statement

1.1. University Canada West ("**UCW**") makes Information Technology Resources available to authorized Users and to assist them in carrying out their work or studies at UCW.

1.2. This Policy establishes rules and responsibilities for the use of Information Technology Resources.

2. Purpose

2.1. The purposes of this Policy are the following:

2.1.1. further the mission and goals of UCW;

2.1.2. ensure that Users comply with applicable laws;

2.1.3. ensure that Information Technology Resources are used for proper UCW purposes; and

2.1.4. define prohibited activities.

3. Scope

3.1. This Policy applies to all Users.

4. Definitions

4.1. The following definitions apply to this Policy and the associated Procedure:

Word/Expression	**Definition**
Access Control Systems	means systems that permit physical and digital access to secure areas and resources at UCW.
Computer Hardware	means desktop computers, laptops, servers, and associated peripherals (monitors, keyboards, etc.).

Data Systems and Licensed Resources	includes data centers, cloud services (OneDrive, SharePoint, etc.), learning technologies, and library resources (digital libraries, online catalogues, licensed databases, journals, ebooks etc.).
Generative AI	includes “artificial intelligences ... that are able to produce text, images, etc.” (Cambridge Advanced Learner’s Dictionary, 2024) These tools include, but are not limited to, assistive writing software (such as ChatGPT) as well as detection tools (such as ZeroGPT).

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:
	(a) Access Control Systems;
	(b) Computer Hardware.
	(c) Data Systems and Licensed Resources;
	(d) Mobile Devices;
	(e) Networking Infrastructure:
	(f) Other IT Equipment and Hardware;
	(g) Security Infrastructure;
	(h) Software and Applications;
	(i) Generative AI software and tools;
	(j) Storage and Backup Systems;
	(k) Telecommunications Systems;
	(l) IT Help Desk and support services; and
	(m) All related equipment and infrastructure.

Mobile Devices	includes tablets, smartphones, and other wireless communication tools used for mobile access to UCW’s resources.
Networking Infrastructure	includes wired and wireless networks that enable internet access, data transfer, and communication in UCW facilities (data centers, server rooms, computer labs, IT Helpdesk, etc.)
Other IT Equipment and Hardware	includes video conferencing equipment, audio-visual equipment, computer labs, printers, and scanners.
Personal Use Records	means information or records relating to personal use (personal emails, documents, voicemails, text messages, social media use, etc.).
Security Infrastructure	includes firewalls, antivirus software, intrusion detection systems, and other tools to safeguard the network and data.
Sensitive Information	includes: (a) personal information (as defined in *PIPA*) of students, staff, faculty, or other individuals (student records, educational records, employment files, etc.); and (b) confidential information about UCW and its business, employees, students, operations, programs, or plans that is not generally known, used, or available to the public.
Software and Applications	includes software applications used for administrative purposes (student information systems, finance systems, etc.), academic purposes (learning management systems, research software, etc.), and communication (email clients, video conferencing, etc.).

Storage and Backup Systems	means hardware and software applications used for supplementary, off-device storage of files and application data (external hard drives, USB drives, cloud storage, etc.).
Telecommunications Systems	includes telephones, voicemail systems, and unified communications tools to enable internal and external communication.
Users	means all students, employees, and other persons who use Information Technology Resources, whether on campus, at other UCW facilities, or remotely.

5. User Responsibilities

5.1. Users are expected to conduct themselves reasonably and to exercise responsible judgment in the use of Information Technology Resources including:

5.1.1. comply with third-party software and information resource license agreements and intellectual property rights;

5.1.2. use Information Technology Resources solely for authorized UCW purposes;

5.1.3. refrain from engaging in prohibited activities under this Policy and the associated Procedure;

5.1.4. seek to uphold UCW's reputation and resources by avoiding irresponsible or illegal actions;

5.1.5. report any observed misuse or security concerns; and

5.1.6. abide by the institutional guidelines for the use and citation of Generative AI.

6. Prohibited Activities

6.1. Users are strictly prohibited from creating, transmitting, distributing, forwarding, retrieving, downloading, uploading, or storing any software, communication, or content that:

6.1.1. is obscene, sexually explicit, or pornographic;

6.1.2. is defamatory, hateful, or constitutes a threat or abuse;

6.1.3. bullies or harasses the receiver, whether through language, frequency, or size of message(s);

6.1.4. is junk mail, spam, or chain email;

6.1.5. forges or misrepresents the sender’s identity; and

6.1.6. divulges personal or confidential information related to UCW.

6.2. Users are also strictly prohibited from undertaking the following activities:

6.2.1. using personal e-mail account for UCW business;

6.2.2. using personal Storage and Backup Systems for the use, storage, or transfer of Sensitive Information or for UCW business;

6.2.3. systematic downloading of licensed content in violation of license agreements or copyright or installing unauthorized programs or software to Computer Hardware;

6.2.4. viewing or accessing obscene, pornographic, or otherwise inappropriate websites using Information Technology Resources;

6.2.5. gaining or attempting to gain unauthorized access to an account on a UCW system; and

6.2.6. initiating mass communications to Users without authorization to listservs, forums, discussion boards, social media sites, or other venues, provided either by UCW or third parties, that segments of the UCW community have knowingly joined.

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

6.3.1. destroying, altering, overriding, overloading, dismantling, disfiguring, or disabling Information Technology Resources;

6.3.2. attempting to circumvent security controls;

6.3.3. knowingly introducing malware including viruses, worms, Trojan horses, and spyware;

6.3.4. intercepting or examining the contents of messages, files, communications, accounts, or programs without appropriate authorization; and

6.3.5. engaging in any uses that result in the unauthorized examination, interception, dissemination, destruction, loss, theft, or alteration of another User's information.

7. Use of Sensitive Information

7.1. Where Sensitive Information is being collected, stored, processed, transferred, or otherwise used:

7.1.1. employees may only access and store Sensitive Information on Information Technology Resources. If an employee must store Sensitive Information on personal computers or mobile devices, the employee must ensure that files are encrypted;

7.1.2. unless approved by their supervisor, employees may not use cloud-based services to store, access, or transmit Sensitive Information on Information Technology Resources;

7.1.3. when using online tools, employees must ensure that they are connected to a private and secure Wi-Fi network (not a public network); and

7.1.4. employees must not use personal email accounts for storage, transmission, or disclosure.

8. Monitoring and Access

8.1. UCW has a responsibility to ensure that all email, communications, data, and information used, downloaded, viewed, accessed, created, or altered using Information Technology Resources comply with UCW's policies, agreements, and laws.

8.2. UCW does not engage in ongoing monitoring of Users' use of Information Technology Resources.

8.3. Regular monitoring may occur for legitimate reasons, including troubleshooting, and addressing network security, performance, system maintenance needs.

8.4. Information stored on Information Technology Resources may also be monitored or accessed by UCW for the following purposes:

8.4.1. to investigate incidents or allegations of misconduct;

8.4.2. to ensure business continuity in exceptional circumstances; and

8.4.3. to ensure compliance with this Policy and laws.

8.5. UCW does not guarantee User privacy in the use of any of Information Technology Resources, including incidental personal use as defined below. UCW may inspect any information or materials stored, transmitted, or created using Information Technology Resources.

9. Incidental Personal Use

9.1. UCW email accounts are to be used only for UCW business.

9.2. Information Technology Resources must not be used for any purpose that is not specifically related to UCW business, except for incidental personal use that:

9.2.1. is infrequent and of short duration;

9.2.2. occurs outside of working hours;

9.2.3. complies with this Policy and all applicable laws;

9.2.4. does not expose UCW to any cost, harm, risk, loss, or liability; and

9.2.5. is not intended for commercial purposes or personal profit.

9.3. UCW cannot guarantee that Personal Use Records will be retained within Information Technology Resources or will remain confidential. Users who utilize Information Technology Resources to create, store, or circulate Personal Use Records do so at their own risk.

10. Policy Contravention

10.1. Users who fail to comply with this Policy may be subject to:

10.1.1. for employees, disciplinary action up to and including suspension or termination of employment;

10.1.2. for students, disciplinary action up to and including suspension; and

10.1.3. for Users, revocation, or suspension of the User's access to any or all of Information Technology Resources.

11. Responsibility

11.1. This Policy is administered under the authority of the Vice President, Operations & IT, who is responsible for the maintenance of this Policy and the associated Procedure.

12. Related Policies

Policy Number	Policy Title
5006	Academic Integrity
6006	Copyright
6751	Information Privacy and Security
8001	Respectful Workplace
8003	Standard of Conduct
9014	Student Rights and Responsibilities

13. Related Procedure

Procedure Number	Procedure Title
2700p	Acceptable Use of Information Technology Resources