CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
OP.604	**Vice-President Finance and Administration**		
Policy Name			
Acceptable Use and Security of Electronic Information and Technology			
Approved by	Replaces	Category	Next Review
SLC	**E.704; ARM1122; ARM1118; ARM1123; ARM1124**		**2023**
Date Issued	Date Revised	Related Policies, Reference	
November 7, 2018		**S2003-01 Academic Freedom** **OP.601 Website** **OP.605 Email for Students, Employees, Alumni and Emeriti** **B.511 Discrimination, Bullying and Harassment Policy** **B.601 Copyright** **B.310 Protected Disclosure (Whistleblower)**	

1. PURPOSE

1.1. Capilano University provides Information and Technology (IT) resources to University users to support the teaching, learning, research and administrative goals and functions of the University. These IT resources are valuable community assets which are expected to be used and managed responsibly to ensure their integrity, security and availability for the educational and administrative activities of the University.

1.2. This policy articulates both acceptable and unacceptable uses of IT resources, thereby ensuring a stable, effective and efficient operation while minimizing potential disruption and risk.

2. DEFINITIONS

"Information and Technology (IT) resources" refer to any University information processing systems, services, infrastructure or the physical locations housing them. This includes computer labs, classroom technologies, computing and electronic communication devices, and services such as modems, email, networks and telephones.

"**Users**" mean all members of the University community, board and senate members, and any other individuals, including the general public, who use University IT resources.

3. SCOPE

This policy applies to:

a. All University owned or controlled IT resources (as defined in section 2) including networks, information systems, applications, computing and communication devices and information assets.

b. Any member of the University community including students, employees and other individuals or organizations that uses University IT resources on or off campus, including student residence.

c. The use of non-institutional equipment connected to the University's networks (e.g. personal cell phones or laptops).

d. User generated content through online publishing and discussion including websites, blogs, wikis, file-sharing, user-generated video and audio, virtual worlds and social networks.

4. POLICY STATEMENT

4.1. The University is committed to the principle of academic freedom (see S2003-01). This policy will be interpreted in that context.

4.2. The University is committed to ensuring a working and learning environment in which all persons treat each other with humanity and respect.

4.3. IT resources provided at the University are primarily intended for teaching, learning, research and administrative purposes. Their use is governed by all applicable University policies, including the B.511 Discrimination, Bullying and Harassment Policy, as well as by all Canadian federal, provincial and local laws and statutes, including the *Criminal Code of Canada*, *Canadian Anti-Spam Legislation* (CASL), the *BC Civil Rights Protection Act*, the *BC Freedom of Information and Protection of Privacy Act, Copyright Act* and the *BC Human Rights Code*. These are supplemented by the acceptable use policies established by those networks to which the University network is interconnected, for example the Internet and BCNet.

4.4. The user bears the primary responsibility for the material that they choose to access, send, display or store. IT resources may not be used in any manner which contravenes the above policies, laws or statutes. The user must use IT resources in a responsible way. This requires that the user:

a. Respect the legal protection provided by copyright and license to programs and data;

b. Respect the rights of other by complying with University policies regarding intellectual property;

c. Respect the privacy and confidentiality of others by not tampering with their data, files, passwords, or accounts, or representing others when messaging or conferencing;

d. Use only network or system IDs or accounts or accounts and communication resources which users are duly authorized to use, and use them for the purposes for which they are intended;

e. Respect the integrity of computing systems and data; for example, by not intentionally developing programs or making use of already existing programs that harass other users, or infiltrate a computer or computing system and/or damage or alter the software or hardware components of a computer or computing system, or gain unauthorized access to other facilities accessible via the network.

4.5. Users have no expectation of privacy when using the University's IT resources.

4.6. The University owns its IT resources and is responsible for its use. The University reserves the right to take action to ensure that its IT resources are used lawfully, appropriately and efficiently in the pursuit of the primary purposes of the institution.

4.7. Employee use of IT resources for any commercial activities must be authorized by the University.

4.8. Incidental personal use refers to use of IT resources that is of a personal nature but that is brief and occasional. Incidental personal use by students and employees is acceptable to the University as long as it does not interfere with the use of University resources for their intended purposes and, in the case of employees, as long as it does not interfere with their job performance.

4.9. Users are prohibited from accessing other users' network or system IDs or accounts and communications capabilities.

4.10. Users are responsible for all uses through their own electronic accounts and must not share passwords to any accounts to which they have access.

4.11. Violations of this policy will be subject to the full range of disciplinary actions available to the University. Proceedings for violations that could lead to disciplinary action will be conducted in accordance with the relevant University policies and/or collective agreements. These include, but are not limited to, B.701 Student Code of Conduct, B.506 Standards of Conduct, staff and faculty collective agreements, and relevant legislation (see section 4.3).

4.12. Initial use of any University IT resource denotes that the user has read and understands and accepts the terms of use outlined in this policy.

5. ILLEGAL AND UNACCEPTABLE USES

5.1. The following, while not exhaustive, provides examples of illegal and unacceptable uses of the University's IT resources:

5.2. Illegal Uses:

a. Uttering threats by any electronic means;

b. Distributing pornography to minors – pornography defined as printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate erotic rather than aesthetic or emotional feelings.

c. Child pornography;

d. Pyramid schemes – defined as a non-sustainable business model that involves the exchange of money primarily for enrolling other people into the scheme;

e. Making unauthorized copies of propriety software or offering unauthorized copies of proprietary software to others;

f. Infringement of copyright, trademark or other intellectual property rights;

g. Installing software that the University has not purchased or using expired trial versions of software.

5.3. Unacceptable Uses:

a. Seeking information on passwords or data belonging to another user;

b. Copying someone else's files or programs or examining such information unless authorized;

c. Attempting to circumvent computer security methods or operating systems;

d. Maliciously downloading files that could potentially damage the University's IT resources;

e. Intercepting or examining the content of messages, files or communications in transit on a voice or data network;

f. Interfering with the work of other users of a network or with their host systems (e.g. chain letters or spamming) or engaging in any uses that result in the loss of another user's files or systems;

g. Using University-provided computer accounts for commercial purposes such as promoting profit-driven products or services;

h. Harassing, defamatory, derogatory, discriminatory or false voice or data messages;

i. Sending, receiving or accessing offensive, objectionable, abusive, pornographic, obscene, sexist, racist, harassing or provocative messages, images or other materials or links. This does not apply to the use of such material in the course of conducting scholarly research;

j. Gambling or betting;

k. Cryptocurrency mining;

l. Political activities;

m. Unauthorized solicitation of funds (e.g. unauthorized solicitation for commercial or profit driven purposes);

n. Unauthorized disclosure of confidential or privileged information;

o. Unauthorized use of data encryption.

6. RIGHTS OF AUTHORIZED EMPLOYEES

6.1. The Vice-President, Finance and Administration may authorize employees to do the following:

a. Take whatever appropriate measures are required to ensure the integrity and availability of the University's IT resources. This includes temporary or permanent accounts and systems access ban or removal of administrative access.

b. Remove material stored on the University's information systems and networks in a timely manner if it is found to be in violation of section 5 of this policy.

c. Carry out an investigation to determine if a user is acting in violation of the policies stated in this document. Employees carrying out such an investigation have an obligation to maintain the confidentiality of a user's files, data and mail.

6.2. Employees who are responsible in the normal course of their duties have the right to examine files, data and mail in order to gather sufficient information to diagnose and correct system hardware and software problems.

7. REPORTING AND INVESTIGATION

7.1. Every employee has an obligation to report any information that is relevant to the safety and security of the University IT infrastructure and/or its students and employees.

7.2. If the violation constitutes a breach of federal, provincial, local laws or statutes, law enforcement agencies will also be notified.