CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
B.604	**Vice-President Finance and Administration**		
Policy Name			
Acceptable Use and Security of Digital Technology			
Approved by	Replaces	Category	Next Review
Board	**OP.604 Acceptable Use and Security of Digital Information and Technology**	**IM&DT**	**June 2027**
Date Issued	Date Revised	Related Policies	
November 7, 2018	**June 25, 2024**	**B.506 Standards of Conduct** **B.511 Discrimination, Bullying and Harassment Policy** **B.700 Privacy and Access to Information Policy** **B.701 Student Code of Conduct** **OP.608 Password Policy**	

1. PURPOSE

1.1 Capilano University (“the University") provides Digital Technology resources to Members of the University Community to support the teaching, learning, research and administrative goals and functions of the University. Digital Technology resources are valuable community assets which are expected to be used and managed responsibly to support the activities of the University, consistent with the University’s purpose and values.

1.2 This policy sets out responsibilities to protect and articulates unacceptable uses of Digital Technology resources, with the intent to provide stable, effective, and efficient operations while minimizing potential disruption and risk.

1.3 The Associate Vice-President Digital Technology Services will develop and maintain a set of Digital Technology standards to support this policy, these standards will be made available on the Digital Technology Services pages of the Frontlines website.

2. DEFINITIONS

“Digital Technology Security Standards” means the formal documentation produced to govern the use and protection of the University network and data.

"Digital Technology resources" refers to the University network and any University-owned or controlled information processing systems, services, applications, infrastructure or the physical locations housing them. Digital Technology resources include computer labs, classroom technologies, computing and electronic communication devices and Information assets including those created for University websites and social media.

"Information asset" means a collection of knowledge or data that is organized, managed and valuable.

"Member of the University Community" means employees, students, board members and volunteers.

"Privileged Access" means having special access to information or systems or abilities to perform functions above that of a normal User. Privileged access is granted on the basis of the individual's role for the sole purpose of completing work-related activities.

"**Social media**" means Internet-based, electronic communications channels through which users create online communities to share and consume information, ideas, images and other content.

"University network" refers to any technology system or service provided by the University**.**

"Users" mean all Members of the University Community, and any other individuals, including the general public, who use University Digital Technology resources.

3. SCOPE

3.1 This policy applies to all University-owned or controlled Digital Technology resources and includes the use of personally-owned equipment (for example laptops or personal mobile devices connected to the University network and/or being used to access University systems, services, applications and infrastructure).

3.2 This policy is not intended to affect the activities of employees and their freedom to conduct and share research and other professional, academic and scholarly work.

4. POLICY STATEMENT

4.1 The University is committed to providing a welcoming, respectful and safe working and learning environment that allows for full and free participation of all Members of the University Community.

4.2 Digital Technology resource use is governed by all applicable University policies, including B.511 Discrimination, Bullying and Harassment Policy, and B.700 Privacy and Access to Information Policy as well as by relevant Canadian federal, provincial and local laws and statutes, and supplemented by the acceptable use policies established by those networks to which the University network is interconnected, for example our Internet Service Providers (ISPs) and BCNet.

4.3 Users bear the primary responsibility for the material that they choose to access, send, display or store. Digital Technology resources may not be used in any manner which contravenes the above policies, laws or statutes. Users must use Digital Technology resources in a responsible way. This requires that Users:

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, including on Intellectual property and privacy protection;

c) Use only network or system IDs or accounts and communication resources which the User is authorized to use for the purposes for which they are intended;

d) Respect the integrity of computing systems and data.

4.4 Digital Technology Services resources are to be used for authorized purposes. Brief and occasional reasonable personal use of Digital Technology resources by students and employees is acceptable to the University, provided it does not compromise the security of, or interfere with the use of IT resources for their intended purposes and, in the case of employees, does not interfere with their job performance. The use of Digital Technology resources for third-party benefit will only be permitted if that use does not create the perception of conflict or interest of commitment as per B.517 Conflict of Interest Policy and with express authorization from a University Administrator.

4.5 Users are responsible for all uses through their own electronic accounts and, in compliance with OP.608 Password Policy, must not share passwords to any accounts to which they have access.

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

4.7 Digital Technology Services resources are to be purchased by Digital Technology Services or with the authorization of the Associate Vice-President Digital Technology Services or their delegate in accordance with B.313.1 Procurement Procedure. Any privately-owned software installed by a User is the responsibility of the User and may be removed without warning if it compromises University security or operations.

5. USER PRIVACY AND CONFIDENTIALITY

5.1 The University owns its Digital Technology resources and is responsible for their use. The University reserves the right to take action to make sure its Digital Technology resources are used lawfully, appropriately and efficiently in the pursuit of the primary purposes of the institution.

5.2 The University respects Users' reasonable privacy expectations for information stored on the University network. Normally Users can expect that their communications and the content of their accounts will be treated as private and confidential and that their files will not be accessed without their permission. However, Users should be aware that they should not expect absolute privacy when using the University's Digital Technology resources.

5.3 Privacy does not apply when Digital Technology Services employees with Privileged Access:

a) collect and use aggregate non-confidential user account data (for example, data that indicate the amount of storage being used by particular accounts);

b) monitor levels of network traffic, use software that logs network activity, make copies of files, and maintain archives of these copies;

c) access files, data, programs, or email in order to gather sufficient information to diagnose and correct network, hardware and software problems. (See also the responsibilities outlined in Section 6.3, below); and.

d) support investigations as described in section 7 of this policy and detailed in the Digital Technology Security Standard Accessing Digital Accounts or Records.

6. ILLEGAL AND UNACCEPTABLE USES

6.1 The following list, while not exhaustive, provides examples of illegal and unacceptable uses of Digital Technology resources.

6.2 Illegal Uses:

a) uttering threats by any electronic means;

b) engaging in online child or youth sexual exploitation including viewing or distributing child pornography;

c) committing fraud or running pyramid schemes (non-sustainable business models that involve the exchange of money primarily for enrolling other people into the scheme);

d) making unauthorized copies of propriety software or offering unauthorized copies of proprietary software to others;

e) infringement of copyright, trademark or other intellectual property rights; and

f) installing unlicensed software or using expired trial versions of software; or

g) breach of any other applicable law.

6.3 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 without authorization;

c) destroying, altering, or disabling files, programs, software and information without authorization;

damaging or altering the hardware or physical components of Digital Technologies without authorization

d) attempting to circumvent computer security methods or operating systems;

e) maliciously downloading files that could potentially damage Digital Technology resources;

f) intercepting or examining the content of messages, files or communications in transit or at rest on a voice or data network without authorization;

g) interfering with the work of other Users 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;

h) using Digital Technology resources for commercial purposes, to promote profit-driven products or services, for unauthorized solicitation of funds, goods or services, for political campaigns or activities, or for any other use that benefits personal or third-party interests above University interests;

i) using Digital Technology resources to intentionally spread false information or information intended to misinform, manipulate or cause harm;

j) sending, receiving or accessing offensive, objectionable, abusive, pornographic, obscene, defamatory, derogatory, discriminatory, harassing or provocative messages, images or other materials or links with the exception of materials accessed or shared:

   i) in the pursuit of legitimate scholarly study or research; or

   ii) as a part of authorized job duties or for an approved investigation.

k) gambling or betting;

l) cryptocurrency mining;

m) unauthorized disclosure of confidential or privileged information; or

n) unauthorized use of data encryption;

7. RESPONSIBILITIES

7.1 The Associate Vice-President Digital Technology Services is responsible for:

a) providing guidance on compliance with the policy;

b) providing ongoing security training to the members of the university community;

c) assisting, where appropriate, in the investigation of breaches and potential breaches of the policy;

d) developing and issuing the Digital Technology Security Standards, which must be consistent with this policy;

e) publishing the Digital Technology Security Standards on the University's internal website for access by all Users;

f) reviewing and updating the Digital Technology Security Standards on an annual basis and

g) leading the coordination of activities aimed at mitigating information security risk, coordinating investigations when information security incidents occur and making sure that appropriate action is taken in response.

7.2 The Associate Vice-President Digital Technology Services will establish protocols for and authorize specific Digital Technology Services employees with Privileged Access rights to do the following:

a) take appropriate measures to safeguard the integrity, confidentiality and availability of the University's Digital Technology resources;

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 investigation to determine if a user is acting in violation of the policies stated in this document as set out in the Accessing Electronic Accounts or Records Standard.

c) examine files, data, and mail in order to gather sufficient information to diagnose and correct system hardware and software problems.

7.3 Individuals with Privileged Access must not access information without authorization and not necessary for their role and are accountable for ensuring the confidentiality of the information they have access to is maintained.

7.4 Administrators are responsible for making sure this Policy is understood and complied with within their faculties and departments and that all faculty or department members complete mandatory cyber security training.

7.5 All Users are responsible for the manner in which they use Digital Technology Resources and for completing mandatory cyber security training when instructed.

8. REPORTING AND INVESTIGATION

8.1 Employees have an obligation to report breaches of this policy and any information about threats to the safety and security of the University network to the Digital Technology Services department. Concerns about employee or student behaviour associated with the use of Digital Technology Resources should additionally be reported to the relevant Administrator, Human Resources or Student Affairs in accordance with the appropriate policy (refer to Section 9).

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

8.3 Investigations under this policy will follow the Investigations Involving Accessing Digital Accounts or Records Standard and as appropriate B.506 Standards of Conduct Policy, B.511.1 – Student Code of Conduct Procedure or other relevant conduct or investigative policies or procedures developed by the University.

8.4 Sanctions under this policy may include temporary or permanent removal of access to accounts and systems or removal of administrative access. Access may also be limited during the investigative period if determined necessary.

9. DESIGNATED OFFICER

The Vice President, Finance and Administration is the Policy Owner responsible for the oversight of this Policy. The Administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Associate Vice President Digital Technology Services.

10. RELATED POLICIES AND GUIDANCE

B.217 Fraud Prevention and Investigation Policy

B.310 Protected Disclosure (Whistleblower)

B.506 Standards of Conduct

B.511 Discrimination, Bullying and Harassment Policy

B.517 Conflict of Interest Policy

B.601 Copyright

B.701 Student Code of Conduct

OP.608 Password Policy

OP.609 Website and Digital Channels

B.313.1 Procurement Procedure

Digital Technology Security Standard - Accessing Digital Accounts or Records.

11. REFERENCES

Criminal Code of Canada,

Canadian Anti-Spam Legislation (CASL)

BC Civil Rights Protection Act

BC Freedom of Information and Protection of Privacy Act,

Copyright Act

BC Human Rights Code

Canadian Centre for Cyber Security