Policy Name:	ACCEPTABLE USE OF INFORMATION RESOURCES
Approved By:	Board of Governors
Approval Date:	June 10, 2025
Next Scheduled Renewal Date:	May 2030
Policy Holder:	VP, Corporate Services & CFO
Operational Lead:	Director, Information Technology/CIO
Policy Number:	INF-001

ACCEPTABLE USE OF INFORMATION RESOURCES POLICY

1.00 PURPOSE

1.1 The purpose of this policy is to define Coast Mountain College's (the College's; CMTN's) expectations and requirements for the use and management of College information technology resources.

2.00 DEFINITIONS

2.1 The following definitions apply in this policy:

a. **College Community:** All employees, students, the Student Union, and the College Board members.

b. **User-Generated Content:** Any form of content created by users (e.g., text documents, images, videos, audio).

3.00 GUIDING PRINCIPLES

3.1 College information technology resources are to be used primarily for activities related to the mission of the College, including but not limited to teaching, learning, research, and administration.

3.2 Users who require access to a computer will be assigned devices as per the Information Technology (IT) standard device allotment.

3.3 Limited personal use is permitted provided it complies with this policy, does not compromise College operations, does not increase costs, does not expose the College to additional risks, and does not unduly impact academic and business activities.

3.4 Use of information technology resources for fraudulent, harassing, threatening, obscene, or malicious purposes is strictly prohibited.

3.5 Use of College information technology resources for personal commercial purposes is prohibited unless authorized by the Director of IT & CIO.

3.6 Users must respect intellectual property, copyrights, and software licensing agreements.

3.7 Use of College information technology resources, including electronic identities, is permitted only for members of the College community and guests.

4.00 SECURITY AND COMPLIANCE MEASURES

4.1 Users must stay within their authorized limits and refrain from attempting to gain unauthorized access to IT resources.

4.2 Any individual using IT resources to create, access, transmit, or receive College-related information must protect that information in a manner that is commensurate with its value, use, and sensitivity.

4.3 Users must respect the rights of others by not encroaching on their access, privacy, or system integrity.

4.4 The College will protect information against unauthorized disclosure.

a. College IT staff reserve the right to access, monitor, and record data usage and storage when there is suspected or alleged impropriety, a business need for access in the absence of an employee, or as required by law.

4.5 Automatic email forwarding to external accounts by all members of the College Community except students is strictly prohibited to maintain custody and control of College records.

a. Students are permitted to use automatic email forwarding to external accounts.

4.6 Unauthorized use of virtual private networks (VPNs) and proxy avoidance tools is prohibited without prior IT approval.

4.7 Users must follow authentication protocols as outlined in INF-004, *IT Password and Authentication Policy*.

a. Credentials, including passwords, must be protected, and access logs may be audited to ensure compliance.

5.00 PROHIBITED ACTIVITIES

5.1 The following activities are prohibited at all times:

a. unauthorized access – attempting to gain access to resources beyond assigned permissions

b. cyber threats – engaging in hacking, denial-of-service attacks (DDoS), or spreading malicious software

c. inappropriate content – storing or sharing obscene, racist, sexist, or defamatory content

d. excessive resource consumption – unauthorized peer-to-peer file sharing or bandwidth-heavy activities that impact College services

e. intellectual property violations – using copyrighted materials without authorization

f. unauthorized commercial use – conducting personal business using College IT resources

g. hosting personal servers or bypassing network restrictions without IT approval.

5.2 Permission for specific research activities may be granted following a meeting with the Dean and the Director of IT & CIO.

6.00 IT LIABILITY AND COLLEGE RIGHTS

6.1 The College is not responsible for user-generated content or damages incurred from IT service disruptions.

6.2 IT reserves the right to:

a. restrict or suspend accounts violating this policy

b. conduct security investigations and audits

c. adjust network bandwidth allocations as needed.

7.00 ENFORCEMENT AND SANCTIONS

7.1 Violations may result in disciplinary action, including suspension of access, or legal action in the event of criminal activity.

7.2 System administrators may immediately revoke access if a security risk is detected.

7.3 Users found in violation of this policy will be subject to investigation under applicable College policies and collective agreements.

8.00 RELATED POLICIES, PROCEDURES, AND GUIDELINES

8.1 ADM-002, *Copyright Policy for Faculty and Staff*

8.2 ADM-009, *Student Non-Academic Conduct Policy*

8.3 HMR-001, *Employee Code of Conduct Policy*

8.4 INF-002, *Cybersecurity Policy*

8.5 INF-004, *IT Password and Authentication Policy*

9.00 OTHER SUPPORTING DOCUMENTS

9.1 BC *Freedom of Information and Protection of Privacy Act* (FOIPPA)

9.2 BC *Human Rights Code*

9.3 *Copyright Act*, Canada

9.4 Canada's Anti-Spam Legislation

9.5 *Criminal Code of Canada*

10.00 HISTORY

Created/Revised/ Reviewed	**Date**	**Author's Name and Role**	**Approved By**
Created	Apr 17, 2018		President's Council
Revised	June 10, 2025	Director of Information Technology & CIO	Board of Governors