


Policy Name:	ACCEPTABLE USE OF INFORMATION RESOURCES	 <p>coast mountain college</p>
Approved By:	President's Council	
Approval Date:	April 17, 2018	
Amendment Date:	N/A	
Policy Holder:	VP Corporate Services	
Policy Number:	ADM-003	
Category:	Administration	

ACCEPTABLE USE OF INFORMATION RESOURCES

1.00 PURPOSE

- 1.01 Coast Mountain College (The College or CMTN) makes computers, communication devices, e-mail, learning management systems (LMS), intranet and internet resources (collectively the "Information Resources") available to authorized users to assist them in performing their work, conducting College business, completing their educational studies and for incidental personal use.
- 1.02 Because the College is a public body governed by the Freedom of Information and Protection of Privacy Act (FOIPPA), records created by using Information Resources are records within the custody or control of the College. All records created and stored on the College's Information Resources may be accessible under this act.

2.00 SCOPE

- 2.01 This policy applies to all employees and students within the College community and to others who have been granted use of the College's Information Resources.

3.00 DEFINITIONS

- 3.01 **Employee:** Any person employed by the College including members of the Board of Governors and contractors.
- 3.02 **Guest:** An individual granted temporary access to the WLAN that is neither an employee nor a student.

- 3.03 **High Volume Data Transfers:** Peer to Peer connections (Video servers such as Netflix or Amazon Prime, BIT torrents, over 100Mb)
- 3.04 **IRC server:** Internet Relay Chat
- 3.05 **Student:** An individual who is registered in a course or program at the College, or not currently registered but living in the dorms.
- 3.06 **WLAN:** Wireless Local Area Network

4.00 POLICY

- 4.01 The College will provide employees and students with a personal, nontransferable, and nonexclusive account, which enables access to the Internet via the College's internet access points.
- 4.02 Installation, operation, and maintenance of all the College's WLAN service shall be the responsibility of the IT Department; the deployment of access that extend beyond the coverage of the College's WLAN service must be approved by the Director of IT.
- 4.03 The College provides access to the World Wide Web and assumes no liability or responsibility for any direct, indirect, incidental, or consequential damages suffered by users in connection with their use of or inability to use information technology services; this includes, but not limited to, damages from loss of data resulting from delays, nondelivery, delivery error and/or service interruptions, or due to inadvertent release or disclosure of information sent by the user. This extends to any affiliates and their respective partners, directors, limited liability company managers, officers, employees, and agents.
- 4.04 The College disclaims to the full extent permitted by applicable law any responsibility and/or liability for any conduct, content, goods, data, and/or services available on or through the internet or the WLAN service.
- 4.05 Use of any information or data obtained via the WLAN service and the internet is at the users own risk, and the College (and its affiliates and their respective partners, directors, limited liability company managers, officers, employees, and agents) disclaims any financial responsibility.
- 4.06 The College reserves the right to conduct periodic maintenance on software and hardware which will result in service interruption. In extenuating circumstances the WLAN service and the Internet may be inaccessible or inoperable for any reason, and the College assumes no liability for damages incurred by these interruptions. The College will make every effort to inform the campus community of scheduled service disruptions.

- 4.07 The WLAN services and Internet are intended for periodic active use of email, instant messaging, browsing the World Wide Web, and other typical end-user activities. High volume data transfers, especially sustained high-volume data transfers, are prohibited. Hosting a web server, IRC server, or any other server is prohibited.
- 4.08 The Library provides streaming resources for academic purposes.
- 4.09 The Internet is to be used for academic and personal use only. Commercial use not authorized by the College is prohibited.
- 4.10 The College is not responsible for the connectivity and performance of privately owned devices. Users shall be solely responsible for maintaining personal devices, ensuring compatibility with the WLAN service, other equipment and/or services required to access and use the service and any lines required for connections.
- 4.11 Users are solely responsible for the security, confidentiality, and integrity of all messages and content they transmit through, or store on the College's information resources.
- 4.12 The College is not responsible or liable, directly or indirectly, for any damage and/or loss caused, or alleged to be caused by, in connection with user access to or transmission of information through the Internet.
- 4.13 Users are solely responsible for maintaining the confidentiality of their account. Users must lock out devices not in use to avoid any unauthorized access to their account by any person. Users will bear all responsibility for use and/or charges incurred from usage of the WLAN service with their password.
- 4.14 Users must conduct themselves in accordance to College Policies and legislation that govern employee and student behaviour.
- 4.15 The College will report any user found in violation of the Canadian Criminal Code and/or CMTN policies; this includes but is not limited to:
- 4.15.1 Transmitting any information or data, in any form, that violates any local, provincial, federal, or applicable international law or regulation, or that is harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, and invasive of another's privacy, and/or hateful (see Sexual Violence and Misconduct, Student Personal Misconduct [E-2015-001] and Employee Code of Conduct [20130415HR]).

- 4.15.2 Engaging in any activity or device in an effort to disguise the origin of any transmission.
 - 4.15.3 Knowingly or willfully transmitting any information or data that contains any computer virus, or any material designed to interrupt, destroy, or limit the functionality of any computer hardware or software.
 - 4.15.4 Any activity that is in the nature of a denial of service attack (DDoS), Hacking and/or port scanning.
 - 4.15.5 Using the information technology services in any fraudulent activity, and engaging in forgery or impersonation.
- 4.16 Users are expected to adhere to the Copyright Act (see Academic Integrity and Appeals Policy [E-2017-004]).
- 4.16.1 Violating or infringing of any copyright, trademark, patent, or other statutory or common law proprietary rights of others.
- 4.17 Users are expected to adhere to the BC Freedom of Information and Protection of Privacy Act (FOIPPA), including the security of any personal information on their device:
- 4.17.1 Using the WLAN Service to collect personal data or attempt to collect personal information about third parties without their knowledge or consent.
 - 4.17.2 Unauthorized release of private/personal and/or confidential information related to the College's business, employees or students.
- 4.18 Users are expected to follow the guidelines in the Canadian Anti-Spamming Legislation (CASL)
- 4.19 Users must conduct themselves in accordance with the BC Civil Rights Protection Act, and the BC Human Rights Code.
- 4.20 Users are expected to adhere to the licensing agreements for all software and hardware licensing agreements.
- 4.20.1 Users are prohibited from reselling access to the College's WLAN Service.
- 4.21 Engaging in any activity that adversely affects the ability of other people or systems to use the WLAN Service or the Internet.

- 4.22 Using information resources to Transmit/Receive P2P, VPN or Proxy Avoidance connections to Non-College servers and services without prior approval.
- 4.23 Violations of this policy will be investigated in accordance with the appropriate conduct policy and collective agreement.
- 4.24 The College reserves the right to suspend accounts from the Internet and deny access to the WLAN service and the Internet at any time, issue warnings (written or verbal), bill users for administrative costs and/or reactivation charges, bring legal action, and/or to collect damages, if any, caused by violations
- 4.25 The College reserves the right, in its sole discretion and without notice, at any time and for any reason, to:
- 4.25.1 Remove or disable access to all or any portion of the WLAN Service;
 - 4.25.2 Suspend user's access to or use of the WLAN Service; and
 - 4.25.3 Reduce the bandwidth available to user.
- 4.26 The College (and its affiliates and its and their respective partners, directors, limited liability company managers, officers, employees and agents) shall have no liability with respect to any claims, losses, or expenses by any party arising out of or relating to:
- 4.26.1 User breach of this Policy;
 - 4.26.2 User use of the WLAN service, including any data or work transmitted or received by users; and/or
 - 4.26.3 Any inappropriate use of the WLAN Service, including, without limitation, any statement, data, or content made or republished by users which is prohibited by this Policy.
- 4.27 The fee (if any) charged by CMTN for your use of this WLAN Service is paid solely for the privilege of accessing this Service. Other websites you visit may charge additional fees.

5.00 RELATED POLICIES & COLLECTIVE AGREEMENTS

- Personal Student Misconduct (E-2015-001)
- Sexual Violence and Misconduct Policy
- Academic Integrity and Appeals (E-2017-004)
- Copyright Policy for faculty and staff (ADM-002)

- Employee Code of Conduct (20130415HR)
- CUPE 2409/FPSE 11 Collective Agreement & FPSE Common Agreement
- BCGEU Local 712 Instructor Collective Agreement & BCGEU Common Agreement
- BCGEU Local 712 Support Staff Collective Agreement
- Excluded Staff Employment Agreements

UNDER REVIEW