Acceptable use of information technology resources

Detailed definitions

Intent:
The intent of this policy is to establish a notion of appropriate use of College Information Technology Resources (ITR) and to establish a framework to assist users in making reasonable decisions regarding acceptable and unacceptable use of college ITR.

Examples of Information Technology Resources:
Acceptable and unacceptable use of College ITR apply to resources the College owns, leases, hosts, maintains, supports or is under legal obligation to manage as a whole or in part. This includes *current and future technology or techniques* used to access college ITR, for example:

Hardware (computer equipment)	Firewalls, servers, computers, laptops, tablets, augmented or virtual reality devices, kiosks, multi-touch surface devices
Software (applications)	Operating systems, ERP, SIS, office productivity software, databases, software as a service
Network (shared resources)	Network addresses, cloud technology, ports, virtual/physical/wireless networks, Internet, Intranet (College Connect), extranet/portals (myBVC)
Security mechanisms	Username, password, identity access card, federated login services, multi-factor authentication, biometrics
Systems	Printers, voice (VoIP & mobile phones), communication (email, social media, Microsoft Teams), video
Business information	Information that supports the College's mandate

Authorized Users:
The College assigns all authorized users a username and password. Users are required to go through the College's authentication processes. Examples of Authorized Users are:

- Registered learners and alumni who are given access to services specific to the user.
- College employees who are given access to services required to support an official role.
- Employees or learners of a partner postsecondary institution where access is dependent on the nature of the partner agreement.
- A third party hired by a College department where access is dependent on the contracted services.
- A confirmed guest of the College e.g. an invited lecturer presenting in the theatre.

Acceptable Use:
Acceptable use of ITR supports college learning, teaching, administration and research activities. Users must:

- Comply with federal, provincial, inter-governmental, and other applicable laws, contracts or licenses, and College policy.
- Use ITR and information the user is authorized for, restrict activities to the intent of the authorization, and respect other users.
- Maintain responsibility for activities linked with the user's account(s) or that originate from ITR under the user's control.
- Protect ITR from damage, loss, or unauthorized access.
- Respect the finite capacity of ITR: Limit use so as not to consume an unreasonable amount of ITR or interfere unreasonably with the activity of other users.

- Use software in compliance with vendor license requirements and with College software standards.
- Use the College's themes (brands) in compliance with College policy, e.g., logos, trademarks, and other images, words, or phrases that represent or are associated with Bow Valley College.

Unacceptable Use
Unacceptable use of ITR involve activities that do not support the College's mandate and/or that could cause harm to a college resource, its business information, to individuals or identifiable groups, or to the College. Unacceptable use includes, but is not limited to:

Illegal activities

- Storing, viewing, displaying, printing or transmitting: copyrighted material, intellectual property or licensed software without permissions; hate literature; child sexual abuse material; or material that could be seen as harassment.
- Sharing another user's login credentials.
- Bypassing or attempting to bypass security controls, e.g., identity masking.
- Unauthorized use of tools to assess security controls or to access a resource, e.g., password crackers, vulnerability scanners, network sniffers.
- Any activity meant to elicit information for the purpose of identity theft, fraud, blackmail or other illegal, malicious or unethical purposes. These activities may include, but is not limited to, the following:
    - **Botnet** creation or distribution is the act of infecting and controlling computers (bots) over a network for the purposes of spreading malicious files or software, infection of further systems, launching Denial of Service Attacks, stealing data, or creating spam campaigns
    - **Cyberstalking or cyberbullying** is the act of threatening or harassing other persons by using communication systems such as email, social networks, and instant messaging applications.
    - **Phishing** is the act of tricking someone into releasing confidential information or into doing something that they normally would not do or should not do.
    - **Spoofing** is an email or other communication that looks like it is coming from a trusted source but is actually coming from an unknown and untrusted source.

Malicious and unethical activities:
These activities may not be illegal; however, these activities may cause harm or may be inappropriate.

- Propagating malware or disrupting services by overloading ITR, e.g., denial of service, downloading large chunks of data, placing a program in an endless loop, excessive printing.
- Unauthorized deletion, modifying, or releasing of business information.
- Commercial, partisan political or personal business activities, e.g., using e-mail to circulate product advertising or to promote political candidates.
- Academic dishonesty, e.g., cheating, plagiarism.
- Continued use of College ITR after the user's relationship with the College has terminated.
- Creating, storing, viewing, displaying, printing or transmitting objectionable material, e.g., pornography, obscenities, graphic violence or language.
- Allowing someone else to use a resource while logged in under your own credentials.
- Sharing your own login credentials.
- Accessing or using information in a way that disregards confidentiality, other users' right to privacy, or College policy, including using a resource while under someone else's login.
- Installing on College ITR software that is not a College software standard.

- Installing on College ITR software that is used for personal monetary gain e.g. crypto mining.
- Connecting to ~~a~~ College ITR without up-to-date antivirus or endpoint protection software.

Capacity:
College ITR are finite, and users are required to use ITR in a manner that does not interfere with other users, or that does not overload or degrade the performance of a College resource. For example:

- Using a resource excessively, e.g. downloading files which impede a resource's performance.
- Using automated processes to gain technical advantage over others using the same ITR.

Incidental personal use:
Incidental personal use restrictions include, but are not limited to the following:

- Usage cannot interfere with the authorized users' or other users job performance or breach acceptable use restrictions.
- The user is responsible for limiting and managing personal use and for any criminal activities or costs incurred as a result of personal use activities, e.g., identity theft, credit-card number theft.
- Understanding that personal use information is susceptible to exposure as part of normal College operations. This includes monitoring and accessing ITR for support, security and privacy reasons, and releasing electronic records when requested by an authorized court of law.

Data sheet

Accountable officer

VP Strategy and CIO

Responsible officer

Lead, IT Security

Approval

President and CEO

Contact area

Information Technology Services

Relevant dates

Approved	Board of Governors: BOG200618-04
Effective	July 2021
Next review	June 2022
Modification history	• Rebranded 2021
Verified by	Office of the President, March 2022*

Associated policies

Academic Honesty (500-1-7)
Applied Research & Innovation Policy (500-3-2)
Building Access Control Policy (300-3-1)
Code of Conduct, Employee and Learner (200-1-13& 500-1-1)
Copyright Policy (500-1-3)
Electronic Communication Policy (300-2-13)
Fraud Policy (200-1-4)
Information Management Policy (300-2-9)
Learner Records & Information Policy (500-1-6)
Learner Appeals (500-1-12)
Print & Imaging Management Policy (300-2-12)
Privacy, Information Security, and Identity Management Policy (300-2-11)
Protected Disclosure Policy (200-1-6)
Records Management Policy (200-1-8)
Technology Management Policy (300-2-7)

Directly related procedures

Electronic Communication Procedure
Employee or Learner Code of Conduct Procedure
Ethical Business Practices Procedure
Protected Disclosure Procedure

Directly related guidelines

Control Objectives for Information and related Technology (CoBIT)

Related legislation

Alberta Human Rights Act
Alberta Evidence Act
Criminal Code of Canada
Freedom of Information and Protection of Privacy Act (Alberta)
Health Information Act (Alberta)