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 technique* used to access college resources, for example:

Hardware (computer equipment)	Firewalls, servers, computers, laptops, tablets
Software (applications)	Operating systems, ERP, office productivity software, databases
Network (shared resources)	Network addresses, cloud technology, ports, virtual/physical/wireless networks, Internet, Intranet (myCampus), extranet/portals (myBVC)
Security mechanisms	Username, password, identity access card, federated login services, multi-factor authentication
Systems	Printers, voice (VoIP & mobile phones), communication (email, social media), 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 resources supports college learning, teaching, administration and research activities. Users must:

- Comply with federal, provincial, and other applicable laws, contracts or licenses, and College policy.
- Use resources 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 resources under the user's control.

- Protect resources from damage, loss, or unauthorized access.
- Respect the finite capacity of resources: Limit use so as not to consume an unreasonable amount of resources 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 resources 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 pornography; or material that could be seen as harassment.
- Sharing another user's login credentials.
- Bypassing or attempting to bypass security, e.g., identity masking
- Using tools to assess security 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 the following:
    - **Pharming** involves Trojan programs, worms, or other virus technologies that attack the Internet browser address bar. When a valid address is typed in, the request is redirected to a fake website instead.
    - **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 computer viruses or disrupting services by overloading resources, 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.
- Continuing to use College resources 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 resources software that is not a College software standard.
- Installing on College resources software that is used for personal monetary gain e.g. crypto mining
- Connecting to a resource without up-to-date antivirus software.

Capacity
College resources are finite, and users are required to use resources 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 resources.

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

- Usage cannot interfere with 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 resources for support and security reasons, and releasing electronic records when requested by an authorized court of law.