ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES POLICY

Policy Statement

Bow Valley College provides Information Technology Resources (ITR) to enable its learning, teaching, administration and research activities. At the same time, the College is obligated to ensure these same resources are used in a secure, effective, reliable, lawful, ethical, and respectful manner. The College, through its policies and its operations, will endeavor to balance these sometimes diverse needs.

Purpose

The intent of this policy is to establish a notion of appropriate use of College ITR and to establish a framework to assist users in making reasonable decisions regarding acceptable and unacceptable use of College ITR.

Scope

This policy applies to all users who access, for any duration, through any means, or from any location, the College's ITR.

Electronic communications and the records transmitted through electronic communications are defined and covered by the Electronic Communications Policy and Procedure.

Principal Objectives

The Acceptable Use of Information Technology Policy of Bow Valley College (the College) will do the following:

1. **Provide a description of what is meant by College ITR, identify roles and responsibilities related to acceptable use of ITR, and establish an understanding that College resources must be used in a way that:**

    - supports Cybersecurity best practices;
    - maintains a stable technology environment;
    - sustains high standards of respectful, ethical and lawful use; and
    - complies with the College's business strategy and policies.

Information resources

1.1 College information resources consists of business information created, stored, viewed, displayed, printed, or transmitted in whole, or in part, using the College's or personal technology resources.

1.2 Business information is information that supports the College's mandate.

1.3 Personal Use information is information that does not support the College's mandate.

Technology resources

1.4 Technology resources are stand-alone or networked computer and telecommunication systems, and current or future technology or techniques used to access College business information.

1.5 A College technology resource is technology the College owns, leases, hosts, maintains, supports or is under legal obligation to manage in part or in whole.

Acceptable use

1.6 Acceptable use identifies how resources can be accessed, who can access them and for what purpose. This includes, but is not limited to:

1.6.1 Users who are granted access to resources according to the College's Authorized User definition.

1.6.2 Use that supports college learning, teaching, administration, and research activities.

1.6.3 Incidental Personal Use as long as it is lawful, ethical, compliant with College policy, and cannot cause Harm to a College resource, to the College or to individuals or identifiable groups.

Unacceptable use

1.7 Unacceptable use identifies how and why resources must not be accessed. This includes, but is not limited to:

1.7.1 Use that either breaches applicable laws, College policy, security controls, or that could cause Harm to the College, College resources, individuals or identifiable groups.

1.7.2 Use that is unethical or disrespectful of other users.

2. Identify roles and responsibilities related to managing acceptable and unacceptable use of resources.

2.1 Executive Management is responsible for governing activities that manage and enforce this policy.

2.2 Human Resources is responsible for managing Employee Code of Conduct Policy 200-1-1 concerns.

2.3 Information Technology Services is responsible for managing its resources in compliance with industry best practices, applicable laws and College policy.

2.4 Learner Services is responsible for managing Learner Code of Conduct Policy 500-1-1 concerns.

2.5 Users are responsible to know and comply with College policy, applicable laws, security controls and ethical norms that govern the use of College resources and to protect resources under their

control from damage, loss, unauthorized access and unauthorized modification of content. They are also responsible for reporting unacceptable use to the appropriate College authority.

3. **Support processes that educate users of the acceptable use of resources.**

4. **Monitor and/or access all College resources, and to restrict or extend access privileges when there are reasonable grounds to do so.**

   4.1 Authorized personnel will perform these activities in the normal course of their responsibilities for the administration and protection of College resources.

      4.1.1 Contents seen are held in confidence except when it becomes necessary to investigate breaches of security, the law or college policy.

      4.1.2 Information that becomes known in these processes will be shared on a need-to-know basis with those responsible for security and the administration of the investigative procedures.

   4.2 The College is obligated when presented with an appropriate order from a competent court to allow access of electronic records to the appropriate authorities.

Severability Clause

If any one of the statements in this document proves to be invalid or unenforceable it will not undo the validity of the remaining statements. The College reserves the right to correct a disputed statement in such a way that it does not modify the overall original intent of the document.

Compliance

Employees, contractors, and learners are responsible for knowing, understanding, and complying with Bow Valley College policies, procedures, and any other attached documentation that relate to their position, employment, or enrolment at the College.

Failure to comply with the Acceptable Use of Information Technology Resources Policy may result in discipline and corrective action.

Use of Bow Valley College ITR is an acknowledgement of this policy.

Definitions

Authorized Users are either users who are granted, through explicit business processes, login credentials and permissions to College ITR, or other users who have a legitimate business reason for gaining access to College resources.

Cybersecurity is the protection against the criminal or unauthorized use of electronic data.

Harm includes, but is not limited to, damaging physical equipment; causing an information technology resource to slow down or be at risk of a security breach, or performing activities that cause unwarranted injury to individuals or identifiable groups, or to the College.

DATA SHEET

Accountable Officer
VP Strategy and CIO

Responsible Officer
Senior Manager IT

Approval
President and CEO

Contact Area
Information Technology Services

Relevant Dates

Approved	May 2018
Effective	July 2018
Next Review	May 2021
Modification History	Approved: President and CEO May 2018

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 (200-1-1 & 500-1-1)
- Copyright Policy (500-1-3)
- Electronic Communication Policy (300-2-13)
- Ethical Business Practices (200-1-5)
- 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)