Electronic communications policy

Policy statement

Electronic communications are an effective means of communicating and delivering important information both internally and externally. Bow Valley College (the College) provides for the exchange of electronic communications while safeguarding its electronic communications systems from inappropriate or illegal use (e.g., reputational damage, spam).

Purpose

The College requires an Electronic Communications Policy to:

- Communicate expectations on appropriate use of the electronic communications systems;
- Protect the College from legal and liability risks and/or reputational damage;
- Ensure compliance with applicable legislation and other College policies;
- Protect the College's visual identity, brand, copyright, trademark, logo; and
- Ensure available, reliable, efficient, appropriate, and optimal use of the College's electronic communications and systems.

Scope

This policy applies to College community members including the Bow Valley College Board of Governors, Executive Management, employees, third party vendors, contractors, and learners. This policy applies to:

- All content transmitted and stored on electronic communications systems owned, managed, operated or contracted by the College;
- All users of College electronic communications systems; and,
- Electronic communications by employees, independent contractors, learners and other individuals associated with the College, where the net impression is that they are representing the College, regardless of whether it is on an electronic communications system owned, managed, operated or contracted by the College. This excludes the use of social media communications, as identified in Social Media Policy 400-3-3.

Principal objectives

1. General

1.1. The College requires electronic communications to conduct its business (core and non-core activities).

1.2. The College determines it's approved electronic communications systems and authorized use of those systems. In particular, the College determines: approval of users; the level of authorization of users; the authority and accountability to create, modify or delete official College social media sites; electronic communications transmitted officially on behalf of the College; and, compliance requirements for independent contractors, including contract language where applicable.

1.3. In addition to what is stated as the purpose of this policy, establishing levels of authority, accountability and compliance requirements is also designed to:

1.3.1. Ensure that electronic communications on behalf of the College, or its departments, accurately and appropriately express the views of the College;

1.3.2. Clarify appropriate use and authority levels of users relative to electronic communications;

1.3.3. Provide that applicable privacy, security and safety standards of individuals are appropriately protected, addressed and mitigated as it relates to electronic communications (e.g., cyber harassment, cyber bullying, reputational damage); and
1.3.4. Ensure that shared information through applicable electronic communications are linked to the original College source online and that any copyright, trademarked materials, and contact information transmitted through official College electronic communications is legally compliant and, where applicable, appropriately acknowledged.

2. Use of Electronic Communications Systems

2.1. College electronic communications systems are intended for business activities of the College. Use is restricted to authorized users.
2.2. Use of the College "Announcements" group email alias is limited to those with specific authority to do so.
2.3. The College may also assign electronic communications accounts to all learners upon enrolment (e.g., myBVC email) conditional on the learner being in good standing with the College.
2.4. In the event College electronic communications systems are used for personal use by authorized users, this Policy (and its Procedure) also applies; users are expected to apply discretion regarding personal use, as per the Acceptable Use of Information Technology Resources Policy 300-2-4.
2.5. Users of the College's electronic communications systems shall not:
2.5.1. Participate in electronic communications intended to deceive or falsify the true identity of the sender, including communications that are anonymous or deliberately forged or that have deceptive material (e.g. inaccurate subject headers);
2.5.2. Impede in any manner the operation of the College's electronic communications systems, including but not limited to unduly incurring unapproved or unbudgeted costs for the College, or any significant or inappropriate costs related to their personal use;
2.5.3. Use or promote materials or communications that are offensive, obscene, indecent, or defamatory including, but not limited to, materials and communications which could result in reputational damage to the College;
2.5.4. Harass or intimidate others;
2.5.5. Act as a representative of the College, or give the net impression of being a representative of the College, without prior authorization or within their level of authority;
2.5.6. Use personal electronic communication systems representing (or on behalf of) the College except where authorized and in compliance with this policy and procedure;
2.5.7. Transmit electronic communications that could cause unwarranted breach of privacy or individual harm by directly or indirectly identifying individuals to specific records or content which is deemed private (Privacy and Access Policy 300-2-10); or
2.5.8. Send commercial electronic messages (CEMs) without the appropriate authority, form requirements, exemptions or consents for compliance with Canada's Anti-Spam Legislation (CASL).

3. Electronic Communications

3.1. "Commercial" Electronic Messages (CEM) are specifically regulated through Canada's Anti-Spam legislation (CASL).
3.2. The majority of the electronic communications the College's authorized users send pertain to the College's core activities (or core business), so are not commercial and are not regulated by CASL. College fundraising is specifically exempted from CASL.

3.3. Users shall follow the College's Electronic Communications Procedure when sending any electronic communications from the College's electronic communications systems (or other systems where applicable).
3.4. The Electronic Communications Procedure defines and outlines processes for:
  3.4.1. Determining what is a CEM, including what is considered core and non-core business activities of the College.
  3.4.2. Electronic communications that involve either core or non-core business activities of the College, which even if not necessarily considered to be commercial in nature (CEMs), require specified compliance, such as approved College signature formats or CASL form requirements;
  3.4.3. Electronic communications that involve non-core business activities, in particular those considered to be commercial in nature (CEMs), that shall comply with CASL (including specific format/form, unsubscribe, and consent requirements);
  3.4.4. Requirements relating to CASL, designed to prohibit spam from electronic communications; and
  3.4.5. Sending group/mass/bulk electronic communications, whether or not commercial in nature (CEMs).
3.5. Except where specified otherwise in this Policy or Procedure, Deans, Directors, and Executive (Level 4 or higher under Delegated Signing Authority Policy 100-2-5) are accountable for group/bulk/mass electronic communications (including newsletters) sent by their departments (or contractors). The accountability includes determining whether: the electronic communication is a core or non-core business activity, it is a CEM, and it is in compliance with this Policy and Procedure.
3.6. The Chief Information Officer, as the accountable executive for this Policy (as well as for legal matters) should be consulted, where appropriate, and has the authority to make the final decision on the sending of group/mass/bulk electronic communications.
3.7. Unless specified or approved otherwise, electronically transmitted newsletters and, where practicable, other group/mass/bulk electronic communications shall utilize approved College software, to ensure unsubscribe and record keeping functionality, whether or not there is a CEM included.

4. Electronic Communications Privacy, Access to Records, Confidentiality and Security

4.1. All records stored on the College's electronic communications systems are subject to the access and privacy provisions of the Alberta Freedom of Information and Protection of Privacy Act (FOIP) and other applicable legislation, including but not limited to Related Legislation on the Data Sheet.
4.2. The requirements and obligations for obtaining express consent under CASL are separate and distinct obligations and differ from the requirements for obtaining consent under FOIP. In using individuals' (e.g., learners and employees) personal electronic communications addresses, users must ensure they comply with FOIP (and the purposes for which the personal information was provided to the College) and CASL.
4.3. Electronic communications records stored on the College's electronic communications systems are governed by the Records Management Policy (200-1-8), the Learner Records Policy (500-1-6), the Information Management Policy (300-2-9), and the Privacy and Access Policy (300-2-10).
4.4. The College does not conduct monitoring of users' content stored on its electronic communications systems, except where warranted by allegations of inappropriate or unlawful use; the College reserves the right to access and/or monitor all electronic communications stored on its electronic communications systems as per the Acceptable Use of Information Technology Resources Policy 300-2-4.
4.5. Users shall comply with authorized and lawful requests from a competent court to search their College electronic communications accounts in order to locate pertinent information.

Pertinent information would be College electronic communications which is relevant to allegations of malicious, unethical, or unlawful use. Users shall not willfully destroy or alter any records with the intent to evade or mislead a request, or any future requests, for access.

4.6. The Chief Information Officer has the authority to establish, and users are expected to follow, additional processes and guidelines related to electronic communications security and usage consistent with this and other related policies and procedures.

4.7. In the event that authorized users receive unsanctioned, inappropriate and uninvited electronic communications on their College electronic communications account, if possible, they should first block the sender or request that the sender cease sending the electronic communications. If the unwanted electronic communications persist, the user should notify the Information Technology Service Desk.

5. Promoting and Securing the College's Identity

5.1. Users representing the College through electronic communications systems shall use the College's approved form requirements. This includes signature format/style/visual identity, as determined by the Vice President, External and CASL requirements determined by the Vice President, Learner Services (see Electronic Communications Procedure).

5.2. Users shall not communicate electronically or give the net impression that they are representing and/or giving opinions on behalf of the College, unless authorized to do so either through an employment relationship (and within one's approved level of authority) or a contract.

5.3. Where users are initiating for the first time an electronic communication, regarding College activities or business, to an individual external to the College, the recommended business practice is that the sender communicate the method that the receiver's electronic contact information was obtained (e.g., business card, website, etc.). Where the electronic communication is a CEM, this practice may be a requirement.

5.4. No one shall utilize College protected copyright and trade-marked materials, including logos, text, photographic images, audio, video, graphic illustrations, computer software and files, in any electronic communications for purposes that are outside the scope of their authority based on their existing employment, contract or learning relationship with the College.

5.5. The Copyright Office within Research and Innovation may be consulted in regard to the dissemination of College copyright and trade-mark protected material transmitted through electronic communications by College or through third parties (Copyright Policy 500-1-3). The content and distribution of protected copyright and trade-marked materials, however, shall not be granted to third parties for their own electronic communications, without prior authorization from the Chief Information Officer.

6. Use of Electronic Communications with Learners

6.1. Employees with the authority to do so may send core business electronic communications to learners (applicants, current learners, and alumni) related to their specific department core business activities, and may use either the learner's "myBVC" electronic communications address or personal electronic communications account, where the latter has been provided by the learner for this purpose.

6.2. Where the learner's personal electronic communications account has been provided as part of the learner's application to the College, consent to use has been provided. The personal electronic communications address provided on the application, however, is subject to a Freedom of Information and Privacy (FOIP) request; therefore, its use is restricted to the purposes for which it was collected (e.g., core business activities outlined on the application). In the case of applicants who do not become enrolled learners, core business electronic communications would relate to their applicant status.

6.3. Prospective learners (who have not applied) may receive electronic communications about core business activities from employees with the authority to do so, for recruitment purposes related to College programs and services.
6.4. Current (or enrolled) learners may receive electronic communications about core business activities. Current learners also have an existing business relationship with the College, under CASL, allowing the sending of CEMs pertaining to the College/learner relationship.
6.5. All credit and non-credit learners who attend the College are automatically considered to be lifetime members of the College community (alumni), once leaving the College and if they continue to be in good standing, regardless of whether they completed or graduated. The College is a not-for-profit entity where consent to send CEMs is not required for members. CASL does still have form and unsubscribe requirements for CEMs sent to college members.
6.6. The personal electronic communications account of a learner, if provided on the learner's application or registration, is considered to be consent to use for electronic communications as the learners become alumni. Alumni programming, for FOIP purposes, is also included in the activities listed on the learner's application. Learners and alumni may also provide personal electronic communications accounts (and updates), through other processes that may be considered appropriate consent.
6.7. Electronic communications from the Alumni Relations department to College alumni members may include information related to entitlements of membership, such as discounts arranged by the College or Alumni Relations for alumni to purchase goods or services from the College or third-party providers. While alumni are lifetime members, and may therefore receive CEMs, they shall, however, be provided with the ability to unsubscribe from electronic communications. Unsubscribing options may include unsubscribing to a newsletter (whether or not the primary purpose is a CEM) or requesting through electronic communications that further CEMs not be sent by a specified College user/sender.
6.8. Electronic communications sent to all current (or enrolled) learners require the approval of the Vice President, Learner Services, (or supervising Executive, President or Acting President). This is to ensure: compliance with this Policy; that the number of electronic messages to all learners is reasonable; and, that it is information that all learners require for conducting the College's business. In the case of emergency electronic communications to learners, other policies may apply with regard to level of authority.
6.9. The Vice President, Learner Services (or supervising Executive) has the authority to send a regular electronic newsletter about core business activities to all current (or enrolled) learners, through the College's student electronic communications system (e.g., Unit4 Business World); and, to do so without including an unsubscribe function.
6.10. All course related activities shall be communicated to learners through electronic communications formats provided by the College Learning Management System (e.g., BrightSpace (D2L), unless where impracticable or not feasible to do so.

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. Non-compliance may create risk for the College and will be addressed accordingly with reference to disciplinary measures considered in the Learner or Employee Code of Conduct Policies and Procedures (200-1-13 and 500-1-1).

Definitions

Access control:
This is the selective restriction of access to a place or resource. Access control over electronic communications refers to usernames and passwords to any electronic communications account, including social media, and to the ability of the College to open and close these accounts, all of which restricts access by authorized users.

Authorized users:
users who are granted, through explicit business processes, login credentials and permissions to College Information Technology Resources (ITR), or other users who have a legitimate business reason for gaining access to College ITR.

Commercial electronic message (CEM):
A commercial electronic message is any electronic communications that encourages participation in a commercial activity, regardless of whether there is an expectation of profit.

Consent:
Consent means a person voluntarily agrees with what is being done or proposed. Consent can be either express or implied according to CASL:

- Express consent is given explicitly, either orally, in writing, or electronically.
- Implied consent involves situations where consent can reasonably be inferred from a past relationship.

Core business:
For the purposes of CASL compliance, the primary area or activity that College was founded on, or approved mandate, and the primary purpose of its operations (see Electronic Communications Procedure).

Dean/Director:
The most senior College employee accountable for an academic or service department. When there is an allegation of inappropriate behavior, "Dean" shall be interpreted as the Dean (or delegate) of the academic department in which an inappropriate behavior occurred; or Director (or delegate) of the service department in which an inappropriate behavior occurred.

Electronic communications:
A transfer of information that is created and sent or transmitted by one or several electronic communications systems to recipients.

Electronic communications systems:
The College authorized or owned telecommunications properties which facilitate the transmission of electronic communications from a sender to a recipient. These electronic transmission methods may include, but are not limited, to:

- Email (myBVC, Unit4 Business World and SMTP);
- Instant messaging (LAN messenger, Microsoft Teams and similar applications or services);
- The learning management system (e.g., D2L);
- Text messages and generated voice mails through College cellular phones, pagers or servers;
- Faxes to and from a College printer and/or other output device;
- College Connect;
- College smart phone applications; and
- College social media accounts.

Employees:
Those who are employed by the College. The College pays employees directly and also files tax information and deductions with the Canadian Revenue Agency.

Group electronic communications:
means group, mass or bulk electronic communications, including newsletters, sent via a College approved tool that includes an unsubscribe mechanism.

Independent contractor:
Businesses, either sole proprietorships or multi-person companies, which provide goods and/or services to the College through a business transaction, are independent contractors. Worker payments, transactions, taxes and benefits are the responsibility of the independent contractor.

Learner:
A person who is currently registered as a learner at the College whether or not for credit. For the purposes of this document, "learner" shall be used synonymously for prospective learners, applicants, current learners and alumni, except where specified otherwise.

- Prospective learner: A person without a formal relationship at the College who is a potential applicant.
- Applicant learner: A person applying for admission to enroll in a credit program.
- Current learner: A person who is enrolled at the College whether or not for credit.
- Alumni learner: All people who were once enrolled at the College whether or not for credit.

Non-core business:
For the purpose of CASL compliance, activities which are not integral or primary to the College's core activities or approved mandate (see Electronic Communications Procedure).

Spam:
Spam is identified as unsolicited commercial forms of electronic communications. Spam includes electronic communications which advertise goods and services that have been sent without the consent solicitation of the recipient, or without a pre-existing relationship between the sender and recipient. The following are identified as spam:

- Address harvesting;
- Chain letters;
- Hoaxes, scams, false warnings;
- Deceptive or intentionally misleading commercial messaging;
- Phishing;
- Smishing;
- Mass communications to electronic addresses without consent or a pre-existing relationship;
- Messages encrypted with spyware, malware or any other type of equivalent; and
- Use of command and control systes, or "botnets".

Trade-marks:
A trade-mark is a word (or words), a design, or a combination of these, used to identify the goods or services of one person or organization.

User:
A person who uses electronic communications. An authorized user is a person who has permission to use the College's electronic communications systems. The individual has an identity which is authenticated through a log in process.

Data sheet

Accountable officer
VP Strategy and CIO

Responsible officer
Lead, IT Security
Executive Member responsible for Marketing and Communications
Executive Member responsible for Human Resources
All Deans, Directors, Executive

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 policy(ies)
Acceptable Use of Information Technology Resources (300-2-4)
Copyright Policy (500-1-3)
Delegated Signing Authority (100-2-5)
Employee Code of Conduct (200-1-13)
Fraud Policy (200-1-4)
Information Management (300-2-9)
Information Security (300-2-11)
Learner Code of Conduct (500-1-1)
Learner Records and Information-Collection, Access and Waivers (500-1-16)
Privacy and Access (300-2-10)
Purchasing Policy (100-1-2)
Records Management (200-1-8)
Violence in the Workplace Policy (200-2-5)

Directly related procedures
Electronic Communications Procedure (300-2-13)
Employee Code of Conduct Procedure (200-1-13)
Ethical Business Practice Procedure (200-1-5)
Learner Code of Conduct Procedure (500-1-1)

Related legislation

Canada's Anti-Spam Act (Canada)
Copyright Act (Canada)
Defamation Act (Alberta)
Electronic Transactions Act (Alberta)
Evidence Act (Alberta)
Freedom of Information and Protection of Privacy Act (Alberta)
Human Rights, Multiculturalism and Citizenship Act (Alberta)
Personal Information Protection and Electronic Documents Act (Canada)
Personal Information and Protection of Privacy Act (Alberta)
Trade-marks Act (Canada)