Confederation
COLLEGE

Policy Title	E-mail
Policy Holder	Senior Director – Computer Services and Project Management
Policy Approver(s)	Senior Team
Related Policies	Acceptable Use of Information Technology Resources Policy (7-1-1) Authorized Access to IT Resources Policy (7-2-1) Non Compliance Penalties (7-2-3) Authentication and Cybersecurity Measursures (7-2-5)
Related Procedures	
Appendices	
Storage Location	Website - https://www.confederationcollege.ca/policies-and-procedures
Effective Date	Oct 28, 2009
Next Review Date	January 30, 2026

Purpose

Confederation College uses e-mail as a primary method of communication. To protect its infrastructure investment and ensure the effective and efficient use of the College's information technology resources, the College regulates the use of its email services.

Scope

The College E-mail Policy applies to all users of College E-mail systems.

Definitions

Phishing	The fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity
SPAM	Unsolicited e-mail sent in large quantities, often used for unethical or potentially harmful purposes.

Governing Laws and Regulations

Policy Statements

1. General

All College students, faculty and staff are assigned an e-mail user account while they maintain a relationship in good standing with the College. The following restrictions apply:

- User accounts are not to be shared; accounts are assigned solely for individual use. Users can however request for the creation of Departmental shared e-mail addresses.

- Individuals are expected to regularly access their College e-mail account to conduct College business and be informed of College events, news, policies, transactions and other information.

- The College e-mail account will be the primary point of contact for individual electronic communications by the College. Third party e-mail accounts can be used to receive information (particularly by students), but the College will default communications to the College assigned account.

- Staff e-mail can be addressed as **First.LastName@confederationcollege.ca** or **useraccount@confederationcollege.ca**. Outgoing staff e-mail will be addressed with the First.LastName format. Student e-mail can only be received by the useraccount@confederationcollege.ca format.

- The College continues to maintain its legacy Internet domain (confederationc.on.ca) for incoming e-mail. Use of this domain is discouraged because of its obsolescence.

- E-mail content must conform to the College's Acceptable Use of Information Technology Resources Policy (7-1-1).

- When staff leave their employment at the College e-mail accounts are maintained according to the Authorized Access to IT Resources Policy (7-2-1).

2. E-mail Distribution Lists

Computer Services creates *E-mail distribution lists* of e-mail addresses of individuals belonging to a specific group. Users request a College e-mail distribution list by contacting the Helpdesk. Requests will be fulfilled for any list that has a College business purpose. The following restrictions also apply:

- Each e-mail distribution list is assigned a staff member who has the responsibility of keeping the list current.

- The College *All Users* distribution list contains the e-mail address of all e-mail accounts of College faculty and staff. The All Users list is intended for use in College wide emergencies, to distribute security bulletins, to announce disruptions to network or server service, and for other important Senior Team information. Other College-wide announcements are to be posted via the College Intranet website/portal.

- The ability to post e-mail to All Users is limited to the President, Vice Presidents, the Director of Communications and Computer Services Helpdesk.

3. E-mail Resources

Computer Services uses a variety of industry-standard methods to ensure continuity of data in the event of equipment failure and to tune system response time. In addition, users are responsible for managing their data as outlined below:

- E-mail messages must be limited in size, particularly when addressed to large audiences. Attachments should be in PDF format or should refer to links to files on College servers for internal audiences.

- Users must purge e-mail folders of older data either by deleting obsolete messages or archiving messages to offline media.

4. Cyber Security Obligations

E-mail is a very popular method for cyber criminals to infiltrate organizations. All users are expected to familiarize themselves with phishing techniques and other social engineering exploits to protect themselves and the College from harm.

- Incoming e-mail with security exploits or obviously offensive content will not be delivered. i.e. email is filtered by the College for malware or spam content.
- All e-mail originating from servers external to the College will be identified as such by the first line of content (inserted by College security hardware/software)
- Web links embedded within incoming e-mail will be scanned for potentially malicious content.

Despite these measures College e-mail users are expected to

- Think and assess before clicking on any link in an e-mail message.
- Be wary of opening any attachments to e-mail, especially unsolicited attachments.
- Use E-mail client software to *Report a Phish* of suspicious e-mail. For more serious or expected widespread phishing call the Computer Services Helpdesk.

E-mail is not to be used to transmit sensitive or confidential information unless the content is encrypted.

Non-Compliance

See 7-2-3 Non Compliance Penalties

Revision History

Version	Change	Author	Date of Change
Original	Original	Paul Inkila	28-10-2009
2		Paul Inkila	18-4-2022