

<b>Title</b>	<b>Electronic Communication</b>
<b>Number</b>	<b>B4002</b>
<b>Category</b>	<b>Administration</b>

## 1. PURPOSE

To define College custody, control and authorized access to the electronic communication system.

## 2. DEFINITIONS

**Chief Information Officer (CIO)** – means the senior administrator in the Information Technology (IT) department of the College.

**Electronic communication system** – includes email, voicemail, digital signage and other forms of electronic communication that are sent by users in the College community. This also includes the College’s social media channels, such as LinkedIn, Facebook, Twitter, etc.

**Electronic mail (email) record** – means any electronic computer record or message created by an electronic mail system.

**Electronic mail (email) system** – means any electronic messaging system, including electronic bulletin boards, discussion lists and newsgroups, that utilize the College’s computing system.

**Enterprise computer technology** – mean all computing and electronic communications resources, facilities, and services that are owned, managed, maintained, or subscribed to by Langara College, both on or off College property that are intended for broad use across the College and/or addresses a strategic goal or objective of the College. This includes, but is not limited to, desktop computers, notebook computers, cloud computing systems, mobile and tablet devices, projectors, flat panel displays, telecommunications equipment, audio visual control systems, data files, telephones, voicemail, computer lab facilities, digital signage, peripheral hardware and software, and the College computer network, including all associated hardware and software, servers, and application software connected to College networks. Computer technology does not include information content or electronic resources for which the Library is the Technical Authority.

**Externally hosted communication channel** – includes the use of a channel that is posted by a third party, such as social media channels, online surveys, email marketing and online collaboration tools.

**Incidental personal use** – means a personal use that does not interfere with a user’s duties or responsibilities and does not interfere with another user’s access to the email system and/or computing system, or create a direct cost to the College. An example of an incidental personal use is sending a short personal email message during an employee’s lunch hour.

**Personal information** – means recorded information about an identifiable individual other than business contact information such as Langara email addresses.

**Senior Leadership Team (SLT)** – the President and the Vice-Presidents of the College.

**User** – means an employee, student, or other individual authorized to use Langara’s electronic communication system. For the purposes of this policy, user includes alumni of the College.

**Voicemail** – means an electronic messaging system that is available to answer telephone calls at any time and record audio messages for playback.

### 3. POLICY

- 3.1 Langara College has custody and control of all electronic mail and voicemail records maintained on the College’s enterprise computing technology. The electronic records and any stored or archived voicemail records are the sole property of the College.
- 3.2 IT staff, authorized by the relevant SLT member and the CIO, or if the CIO is involved, authorized by both the Vice-President, Finance and Administration and the President, may gain access to users’ electronic communications and data, and other materials including, but not limited to, email, proxy and firewall logs, address books, desktop logins and printed emails without the consent of the user in the following instances:
- a) when necessary for the maintenance and security of the electronic mail, voicemail, and/or computing system;
  - b) for re-routing or disposing of undeliverable email;
  - c) when access is required to complete an academic or administrative process where the user is not available or is no longer employed by the College;
  - d) for gaining access to business email and voicemail records where the owner of the mailbox is not available or is no longer employed by the College;
  - e) for compliance with legal requirements to disclose information; or
  - f) when there are reasonable grounds to believe that a violation of law or a significant breach of College policy has taken place.
- 3.3 The College may refuse, filter or discard electronic communications from externally hosted communication channels that are:
- a) unsolicited;
  - b) mass or commercial messages;
  - c) communications that appear to contain viruses;
  - d) messages that include hate speech;
  - e) pornography; or
  - f) any other content that appears to violate College policies or law.
- 3.4 All electronic records may be accessed under the B. C. *Freedom of Information and Protection of Privacy Act*.
- 3.5 Users will not forward electronic communications to any personal accounts or servers, including, but not limited to, personal webmail (such as GMail, Yahoo, etc.) or document storage services (such as Dropbox).
- The B. C. *Freedom of Information and Protection of Privacy Act* does not allow the storage of personal information outside of Canada except under specific circumstances.
- 3.6 All official electronic communications conducted by faculty and/or staff of the College to any students, stakeholders or external individuals and/or groups will be conducted on a communication platform provided by the College. College employees will not cause their official Langara email to be forwarded to any other commercial, private or personal

email provider at any time.

- 3.7 All users will familiarize themselves with Policy B5002 – Computer and Computing System Use, paying particular attention to prohibited and allowed uses, sender identification, password disclosure, and compliance.
- 3.8 Users will manage their electronic communication records in accordance with Policy B5010 – Records and Information Management and its procedures.
- 3.9 It is the user’s responsibility to notify IT immediately if they suspect or know that their credentials (ID and Password) for accessing any electronic technology have been compromised.
- 3.10 The CIO or designate will issue guidelines to update the procedures and user responsibilities.

**Relationship with Other Policies**

- 3.11 Application and/or violation of this policy will be considered in conjunction with the College’s other policies including, but not limited to, the Computer and Computing Use Policy, Student Code of Conduct Policy, Ethical Conduct Policy, Human Rights Policy and Respectful Workplace Policy.

**4. RESPONSIBILITY**

For inquiries relating to this policy, contact the Chief Information Officer.

**5. REGULATIONS/PROCEDURES**

[Electronic Communication Procedures](#)

<b>History/Revision</b>	
Origination Date	January 23, 2007
Amendment Date	February 11, 2020
Next Review Date	February 11, 2023