St. Lawrence College

CR605: BYOD (Bring Your Own Device) Policy

Policy Title:	BYOD (Bring Your Own Device) Policy
Policy Number:	CR 605
Owner:	Chief Information Officer
Approved by:	Corporate Policy Review Panel & SLT
Effective Date:	July 2026
Reference:	Enter text
Links to Other Policy:	Provided in the document. See below.

St. Lawrence College is committed to making our resources fully accessible to all persons. This document will be made available in alternative format upon request.

BACKGROUND

Definitions

- **BYOD (Bring Your Own Device):** Use of a personally owned device to access SLC systems.
- **Personal Device:** Any device not owned, issued, or managed by SLC.
- **Data:** Information in any form (raw or processed) used or stored by SLC.
- **Service:** SLC-provided systems, applications, or technology services.
- **Proctored/Lockdown Exams:** Assessments requiring software, monitoring, or device restrictions.
- **Mobile Device Management (MDM):** Technology used to apply security controls to devices accessing SLC systems.

Purpose: This policy establishes requirements for the secure and appropriate use of personally owned devices when accessing St. Lawrence College (SLC) systems and services. The policy is intended to support flexible teaching, learning, and work environments while protecting college information, maintaining academic integrity, respecting personal privacy, and ensuring compliance with applicable laws, regulations, and contractual obligations.

Scope:

This policy applies to all individuals accessing SLC systems using personal devices, including:

Who:

- All students (full-time, part-time, continuing education)
- All employees (faculty, staff, contract, and part-time)

Devices:

- Laptops, Desktops, Tablets, and Smartphones, and other IOT Devices

Services/Resources:

- Email and collaboration tools
- Learning management systems (LMS)

- Virtual desktops and remote access services
- Licensed software
- Wireless networks
- Digital library resources
- Online assessment and exam platforms

This policy does **not** apply to SLC-owned and IT-managed devices, which are governed by separate college policies. Individuals employed and provided a device by SLC in a student-employee capacity are governed by staff and managed device policies when acting in that role.

POLICY STATEMENTS

General Requirements

Users must comply with all applicable laws and SLC policies when using personal devices to access college systems and services.

Personal devices may be used to access approved SLC services, provided that users:

- Maintain supported operating systems and applications with current security updates
- Use Multi-Factor Authentication (MFA) for SLC accounts
- Access SLC services using valid credentials

Guiding Principles

- Protect the confidentiality, integrity, and availability of institutional data
- Respect the privacy of personal information on user-owned devices
- Ensure compliance with privacy and data protection legislation
- Clearly define shared responsibilities between SLC and the device owner

Acceptable Use

Personal devices used under BYOD may be used to:

- Access approved SLC systems and services
- Support teaching, learning, research, and administrative activities

Personal devices must not be used to:

- Circumvent college security controls
- Store sensitive college data outside approved services
- Engage in illegal or policy-violating activity

Security, Privacy, and Data Protection

Users must ensure that:

- College data is stored only within approved SLC systems and services
- Sensitive college data is not stored on personal devices

SLC may collect limited technical device information (e.g., device type, operating system version, security status) to support secure access.
SLC does not access personal files, applications, or communications on user-owned devices.

Academic Assessment and Exams (Students)

Where required to support academic integrity:

- Students may be required to install and use approved exam or assessment software
- Secondary or wearable devices may be restricted during exams
- Students are responsible for testing device compatibility prior to exam day

Where personal device access presents a barrier, SLC will provide alternative access through established accommodation processes.

Loss, Theft, or Compromise

Users must immediately report lost, stolen, or compromised devices that have access to SLC systems. To protect college data and systems, SLC may suspend access, reset credentials, revoke sessions, or remotely remove college data from a personal device. SLC is not responsible for loss of personal data resulting from these actions.

Support and Maintenance

SLC provides limited support for personal devices, restricted to access to SLC services (e.g., email, WiFi, VPN, LMS). The device owner is fully responsible for:

- Purchasing, maintaining, and repairing the device
- Operating system, hardware, and peripheral support
- Mobile carrier plans, data charges, and accessories
- Backing up personal data

Provision of funding or reimbursement does not imply IT support for the device.

Compliance and Enforcement

Failure to comply with this policy may result in:

- Suspension or termination of BYOD access
- Academic or disciplinary action in accordance with applicable SLC policies, collective agreements, or student codes of conduct
- Further investigation in cases of serious or repeated violations

Exceptions

Exceptions must be documented, justified by academic or operational need, and approved by Information Technology Services and the appropriate authority.

MONITORING

This policy will be reviewed and updated as required to reflect changes in technology, risk, and regulatory requirements.
Continued use of personal devices to access SLC systems and services constitutes acceptance of this policy.

NEXT POLICY REVISION DATE

July 2031

SPECIFIC LINKS

- Acceptable Use of Technology Policy (CR 601)
- Terms Of Service - St. Lawrence College
- Privacy Notice - St. Lawrence College