Selkirk College

Policies and Procedures

Effective: 2024/05/28
Next Review: 2027/05/27
Policy Number: 7110

Acceptable Use of Electronic Resources

A. PURPOSE

Selkirk College is dedicated to ensuring that its employees and students have the necessary technology to maximize their efficiency and improve work processes and learning outcomes. Employees are encouraged to utilize all internal computer-based technology (computer, email, internet, network systems, etc.) to their fullest to fulfill their job requirements effectively.

The purpose of this policy is to outline and ensure that college computer and technology resources are always used appropriately to support Selkirk College and its mission.

College computer facilities, accounts, and services are provided for educational, research, teaching, and administrative purposes. Selkirk College's systems are to be used for appropriate Selkirk College business. Uses that threaten the integrity of Selkirk College systems, the function of non-institutional equipment that can be accessed through the system, the privacy and actual or perceived safety of others, or that are otherwise illegal, are forbidden.

B. SCOPE / LIMITS

This policy applies to all users of the college's computer facilities, accounts, information, internet, and Selkirk College systems.

By using Selkirk College systems, the individual assumes personal responsibility for their appropriate use and agrees to comply with this policy and other applicable Selkirk College policies, as well as city, provincial, federal and/or international laws, and regulations.

With the understanding that Selkirk College is a publicly funded institution and as such is subject to regulatory laws governing the safety, security and privacy of our employees and students, the level of security is defined based upon the needs of both health-and-safety-governing bodies and financial-regulatory bodies.

C. PRINCIPLES

1. All users of Selkirk College computer facilities, accounts, email, cell phones and software systems are responsible for using them appropriately and maintaining their security.

2. College computer facilities and services must be used in a responsible fashion. Using accounts, cell phones, computer facilities, or systems in ways that disrupt others, or interfere with their intended purpose is not permitted.

3. The College reserves the right to secure, inspect, copy, remove, or otherwise alter files in the regular conduct of its duty to maintain efficient, secure, and well-run resources.

4. Single Sign On computer ID and account authentication system provides users with access to a variety of college systems and services. These accounts are issued to a specific user and sharing passwords with others is not permitted. Users are responsible for the security of their password.

5. Users of Selkirk College systems must preserve the security and confidentiality of the information in these systems. The information is to be used only in the course of a work assignment at the college. The information must be kept strictly confidential and cannot be divulged to others except in the performance of college authorized work.

6. Employees must ensure any device, either personal or Selkirk College owned, that contains Selkirk College information or has access to Selkirk College information, is protected (i.e. a screen lock on mobile devices and virus protection).

7. When accessing Selkirk College systems with non-Selkirk owned devices users must adhere to this policy (i.e., do not leave devices unlocked or unattended when accessing Selkirk College systems). Only maintain Selkirk College information on non-Selkirk College owned devices while actively working on it and ensure it has been securely deleted when no longer needed. Selkirk College information must not be stored permanently on devices.

8. The Information Technology Services (ITS) department may access devices and monitor all users of Selkirk College Systems. This includes but is not limited to email and internet systems by monitoring the email server and internet network performance and retained logs, backups and archives and decryption of traffic. These records may be audited, are subject to provincial and/or federal laws, and may be used as evidence. While individual usage is not routinely monitored, unusual or high-volume activities or upon the request of Selkirk College may warrant more detailed examination.

9. Users must not modify, disrupt, or damage Selkirk College Systems either through intent or accident outside the scope of a user’s job duties. This includes but is not limited to:
   - access non-public network with unauthorized equipment;
   - adjusting network configuration including swapping network cables;
   - removing computers;
   - port/network scanning;
   - attempting to access restricted information;
   - introduction of unapproved or malicious software;
   - sending unsolicited email.

10. Users who breach this policy may be subject to disciplinary actions. Selkirk College may also remove or restrict access to any account as required. For students, failure to comply with this policy may result in suspension of computer privileges or other disciplinary action. For employees of the college, the appropriate policies, procedures, and collective agreement provisions on discipline will apply.

11. All user accounts are subject to the account creation and access removal guidelines and timelines, as outlined in the procedure documentation.

12. Users must report instances of misuse or unauthorized activity to the ITS department immediately. Passwords must be changed immediately if an account is compromised or if there is a strong suspicion that it has been compromised.

13. Users must use security and update features (virus protection and Windows updates for example) provided by Selkirk College, as required. If users suspect that their computer is infected by a virus or has been compromised, the users must notify the ITS department to ensure that this is remediated.

14. All systems acquired or purchased by the college for use with Selkirk College systems are the property of Selkirk College.

D. DEFINITIONS

Users: Faculty, staff, administrators, students, contractors, and any other individuals who use Selkirk College facilities, accounts, email, internet, systems, and services. This is often referred to in other policies as the Selkirk College Community.

Accounts: Any password protected login for Selkirk College systems provided by the college, accessed either on campus or remotely, due to studying, working, or being physically present on campus.

Selkirk College Systems: All services, devices, and facilities owned, leased, or provided by Selkirk College and used to store, process, or transmit electronic information. These include, but are not limited to:

- computers and computer facilities, computing hardware, and equipment;
- shared and network drives;
- mobile computing devices such as laptop computers, smartphones, and tablet computers;
- electronic storage media such as USB memory sticks and portable hard drives;
- communication and collaboration software and networks;
- enterprise resource planning software
- third-party cloud solutions;
- email systems;
- telephone and other voice systems; and
- software.

Single Sign-On: An authentication process that allows a user to access multiple applications (i.e. Outlook, Unit4, and SharePoint) with one set of login credentials.

E. LINKS TO RELATED POLICIES

6005 Responsible Use of College Digital Communication Tools, **6550** Protection of Privacy, **6010** Human Rights, **8630** Student Email, **4200** Responsible Use of College Facilities and Equipment, **2505** Social Media

Responsibility, Recommendation and Approval Dates

Executive Responsibility: CFO, VP College Services
Administrative Responsibility: CIO
Recommended by Policy Review Committee or Administrative Policy Review Committee: 2024-04-09
Recommended/Approved by Education Council: n/a
Approved by President:

Maggie Matear
Signature

May 21, 2024
Date