Selkirk College **Policies and Procedures**		Number 7110	Title **Acceptable Use of Electronic Resources**		
		Replaces	NEW		
		Effective	2012-01-19	Next review:	2017-01-19
Executive Responsibility	Administrative Responsibility	Recommended by Policy Review Committee		2012-01-19	
VP Finance and Administration	Director of IT	Recommended/Approved by Education Council		N/A	
		Approved by President		2012-01-20	

1 PURPOSE

This policy defines the boundaries of acceptable use of Selkirk College electronic resources, including but not limited to computers, printer, fax machines, copiers, networks, electronic email services and electronic information sources, as detailed below.

The policy defines penalties for infractions, up to and including loss of system access, fines and employment termination. In addition, some activities may lead to risk of legal liability, both civil and criminal.
Users of electronic information systems are urged in their own interest to review and understand the contents of this policy.

The intent of this policy is not to impose restrictions that are contrary to Selkirk College's established culture of openness, trust and integrity. The college is committed to protecting its employees, students, and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly.

When demand for computing resources exceeds available capacity, priorities for their use will be established and enforced. Information Technology Services (ITS) staff may set and alter priorities for computing/networking resources. The priorities for use of institution-wide computing resources are:

- **Highest:** Uses that directly support the daily business and mission of Selkirk College.
- **Medium:** Other uses that indirectly benefit the business and mission Selkirk College, as well as and including reasonable and limited personal communications.
- **Lowest:** Recreation, personal and all other non-business related activities.
- **Forbidden:** All activities in violation of applicable laws and regulations or prohibited in the section 4.2 of this policy.

ITS may enforce these priorities by restricting or limiting usages of lower priority in circumstances where their demand and limitations of capacity impact or threaten to impact usages of higher priority.

2 SCOPE / LIMITS

This policy applies to employees, contractors, consultants, temporaries, and other workers at Selkirk College including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Selkirk College.

With the understanding that Selkirk College is a publically 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.

The following items take into account the guidelines proposed by and attempt to address, the regulations of

these governing bodies.

- Installation of authorized/standard software/hardware and new software/hardware;
- Physical/logical security of all computer server hardware and equipment;
- Access security of all communication equipment, mobiles communication devices (Blackberry, iPhones, Android, etc.), landlines, dial-up lines and wireless networks;
- User access control (access requests and regular access review);
- Password policies;
- Access, integrity and confidentiality of all end-user workstations, laptops, terminals, printers and related equipment;
- Access authorization and granting process;
- Access security (user access requests, privileged access requests and access privileges) and integrity (modifications) of all system software and application programs;
- Access security and integrity of all databases and other media where data resides;
- Access, confidentiality and integrity of all information stored on electronic media and output (e.g.: paper, fiche, CDs, DVDs, Digital Media, etc.);
- Modifications to system software, applications programs and databases;
- Data classification (inventory of all electronic assets and their ownership);
- Email and internet security;
- Security logs and review policies;
- Sanctions and repercussions of misuse and breaches.

3 PRINCIPLES

This policy is based on the principle that the electronic information environment is provided to support Selkirk College and its mission; all other uses are secondary. Uses that threaten the integrity of the system, 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.

By using Selkirk College electronic information 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, as detailed below.

Internet/intranet/extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Selkirk College. These systems are to be used solely for purposes in serving the interests of Selkirk College, staff and students in the course of normal operations.

Effective security is a team effort involving the participation and support of every Selkirk College employee and student who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

4 PROCEDURE

4.1 General Use and Ownership of Information

While Selkirk College's network administration desires to provide a reasonable level of privacy, users should be aware that, unless expressly agreed upon by both parties, the data they create on the institutional systems remains **the property of Selkirk College**. Because of the need to protect Selkirk College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Selkirk College.

ITS recommends that any information considered sensitive or vulnerable by users be encrypted. For guidelines on information classification and ownership of information, see ***Classification of Information*** as well as ***Ownership Roles and Responsibilities*** documents published by ITS on Moodle. For

guidelines on encrypting email and documents, go to ***ITS' Security Awareness Site.***

For security and network maintenance purposes, authorized individuals within Selkirk College may monitor equipment, systems and network traffic at any time, per ***ITS' Audit Policy*** (available under ITS on Moodle). Selkirk College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Unacceptable Use

The activities listed below are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting services).

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.2.1 System and Network Activities

The following activities are strictly prohibited unless otherwise noted:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Selkirk College;

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Selkirk College or the end user does not have an active license;

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question;

- The introduction of malicious programs into the network, servers and/or individual electronic devices whether local or remote (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);

- Revealing your account name and/or password to others or allowing use of your account by others or any privileged network account to which you have access. This includes family and other household members when work is being done at home;

- Using a company-owned computing asset to actively engage in procuring or transmitting material that is in violation of copyrights, sexual harassment or hostile workplace laws in the user's local jurisdiction;

- The making or transmitting of fraudulent offers of products, items, or services originating from any Selkirk College account or utilizing any company-owned assets;

- Making statements about warranty of electronic assets, expressly or implied, unless it is a part of normal job duties;

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "***disruption***" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

- Port scanning or security scanning;
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty;
- Circumventing user authentication or security of any host, network or account;
- Interfering with or denying network, server and/or internet service to any user or the institution (for example, denial of service attack);
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet/extranet;
- Providing information about, or lists of, Selkirk College employees and/or students to parties outside Selkirk College.

4.2.2 Email and Communications Activities

The following activities are strictly prohibited:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam) and/or posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages;
- Unauthorized use, or forging, of email header information;
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;
- Use of unsolicited email originating from within Selkirk College's networks of other internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by Selkirk College or connected via Selkirk College's network;

4.2.3 Social Media (SM) and Blogging

- Engaging in social media activities, including but not limited to blogging by employees, whether using Selkirk College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Selkirk College's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Selkirk College's policy, is not detrimental to Selkirk College's best interests, and does not interfere with an employee's regular work duties. Blogging from Selkirk College's systems is also subject to monitoring and control.
- Selkirk College's ***Classification of Information*** document also applies to SM activities. As such, employees are prohibited from revealing any company confidential or proprietary information, trade secrets or any other material covered by Selkirk College's ***Classification of Information*** document when engaged in SM activities.
- Employees shall not engage in any SM activities that may harm or tarnish the image,

reputation and/or goodwill of Selkirk College and/or any of its employees or students.

- Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when engaged in SM activities and/or otherwise engaging in any conduct prohibited by Selkirk College policy 6010: ***Human Rights***.

- Employees may also not attribute personal statements, opinions or beliefs to Selkirk College when engaged in SM activities. If an employee is expressing his or her beliefs and/or opinions, the employee may not, expressly or implicitly, represent himself or herself as an official representative of Selkirk College. Employees assume any and all risk associated with SM activities.

- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Selkirk College's trademarks, logos and any other Selkirk College intellectual property may also not be used in connection with any SM activities unless in performance of official duties.

4.3 Adherence to provincial, legal and legislative requirements

The local, provincial, national and international laws (e.g. on data privacy, dissemination of pornography) and regulations must be adhered to. Under no circumstances is an employee of Selkirk College authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing institutional resources.

Privacy laws: Personal data shall be protected according to the data privacy laws of the country where is stored or processed. Due to the federal, provincial and local laws, every effort will be made to retain all data on-site except where required by governing agencies.

Note: Some "Cloud" services such as Dropbox, Evernote and Google Docs reside outside of Canada and are subject to the privacy laws of the hosting sites and/or company headquarters and privacy laws can be substantially different than those enjoyed in Canada.

Disclosure: Information may be compelled from the college through legal processes or through other policies.

5. OTHER RELEVANT POLICIES

6005 Responsible Use of College Email

6010 Human Rights

8630 Student Email