SAMPLE POLICY

ACCEPTABLE USE OF COMPUTER NETWORK

PURPOSE

1. The purpose of this policy is to guide Board of Education employees in the use of Board computers and other equipment and resources including but not restricted to telephones, cellular phones, PDA units and all other devices which have access to or may store information obtained from the Board's computer networks (hereinafter collectively referred to as "the computer network").

2. The policy recognizes the Board's need for secure and effective access to and use of information technology and other resources including the computer network.

POLICY STATEMENT

1. Employees of the Board shall comply with this policy and any related guidelines and directives to enable reasonable and appropriate use of the computer network and all Board resources.

ACCEPTABLE USES

1. Employees who have been granted access to Board computer networks are expected to use such networks in a legal, ethical, collegial and non-destructive manner consistent with a spirit of respect and in accordance with the policies and procedures of the Board and with the laws of Canada and Saskatchewan.

2. Acceptable uses of the Board's computer network shall include but are not limited to:

a) purposes related to the specific functions of each employee's job or purposes required to assist employees in carrying out the duties of their employment;
b) reasonable private purposes which are consistent with this Policy; and
c) those uses set out in *Appendix A* to this policy.

3. Unacceptable or prohibited uses of the Board's computer network shall include but are not limited to:

a) any use by an Employee that significantly interferes with the duties of employment;
b) any use by an employee that exposes the Board to significant cost or risk of liability; and
c) those uses set out in *Appendix B* to this policy.

4. a) The rules set out in this policy provide general guidance and examples of unacceptable or prohibited uses are for illustrative purposes and should not be construed as being exhaustive of unacceptable use.
b) Employees who have questions as to whether a particular activity or use is acceptable should seek further guidance from the Director of Education or designate.

WEB PAGES

1. Material published to the Board website must be approved by the Director or designate

2. Information published must meet the following minimum standards:
a) sources must be cited;
b) information should be as correct and timely as possible.
c) copyright laws apply and copyright notices must be included where appropriate; and
d) privacy consideration should be addressed

MONITORING

1. The computer network is owned by the Board and the Board reserves the right to access the contents of all files stored on the network and all messages transmitted through its computer network.

2. The Board keeps and may monitor logs of usage of equipment which may reveal information such as: (*list those items which the board intends to monitor, for example:)*

- *which internet servers and sites have been accessed by employees;*
- *the email addresses of those with whom employees have communicated; or*
- *the content of communications including emails and instant messages.*

3. Except as otherwise provided for in this policy the Board:
a) will not engage in real-time surveillance of internet or equipment usage; and
b) will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law.

4. Surveillance and disclosure by the Board may take place in the following circumstances:
a) in the case of a specific allegation of misconduct, the Director or designate authorise accessing of such information when investigating the allegation
b) when the IT Support section cannot avoid accessing such information whilst fixing a problem.

5. In cases where information is accessed the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary.

COPYRIGHT

1. All computer hardware and software in use is purchased under academic licenses and there must not be any commercial activity of any kind on Board networks.

2. Software must only be used legally in accordance with both the letter and spirit of relevant licensing and copyright agreements.

SECURITY:

1. Employees shall not attempt to gain unauthorised access to information or facilities. and shall not modify the contents of any computer.

2. Any information that users consider sensitive or vulnerable must be encrypted before being circulated or stored.

3. Employees shall not remove from board premises any laptop, cell phone, PDA, memory key or other storage device, or any other device on which personal or confidential information may be stored or accessed until ensuring that appropriate security measures have been implemented.(See the Board's Security Policy)

4. Every employee must immediately report any possible or suspected breach of security to his or her supervisor who in turn shall immediately notify IT Services.

USERNAMES AND PASSWORDS

1. Employees who require computer network access in order to perform the functions of their employment will be assigned usernames and passwords in order to be able to access required services.

2. Passwords are not to be shared with friends, family or others, except other employees of the Board who require the information for the purposes of their employment, and must be assigned and changed in accordance with guidelines established from time to time by IT Services.

3. Employees will be held accountable for any abuses carried out by unauthorized disclosure of a password.

HARDWARE AND SOFTWARE:

1. All purchases must be approved by the IT Manager, preferably through the IT budget.

2. Permission from the employee's supervisor and IT Services must be obtained before any software (including public domain software) is installed on equipment that is part of the computer network.

3. Prior approval is required for subscriptions to mailing lists and bulletin boards or enrolment by employees on social networking sites and other similar activities.

REMOTE ACCESS

1. Employees are permitted to use remote access to the board computer network subject to the following:

a) access must be strictly controlled, using password authentication as directed by IT Services;

b) it is the responsibility of employees with remote access privileges to ensure that a connection to the Board is not used by non-employees to gain access to Board computer network resources; and

c) the employee must take every reasonable measure to protect the Board's assets and information.

ENFORCEMENT

1. Violating this policy may lead to the immediate denial of access to the computer network or to a particular device or service.

2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPENDIX A
ACCEPTABLE USES

Acceptable uses of the computer network include, but are not limited to, the following:

1. Work-related purposes
a). Unless specifically directed otherwise an employee may use the computer network if access to the computer network is required to perform any portion of work duties assigned to the employee.

b). All work related uses must be in accordance with the terms of this Policy.

2. Incidental Purposes
a). Employee may also use the computer network for reasonable private purposes such as sending and receiving personal messages as long as such usage is consistent with this Policy

b). Employees shall comply with the following rules in any incidental use of Board resources:

- incidental use must not impede the employee's work or the work of others, or affect the Board's ability to carry out its work;
- the personal use is moderate in time;
- the personal use does not incur significant cost for theBoard ;
- employees shall at all times exercise good judgment in the incidental use of Board resources;
- employees shall restrict personal communications during office hours to pressing matters only, and such communications must be brief; and
- employees shall use a personal e-mail address, and shall not send the messages from a Board address;

  (Or: "*postings by employees from a Board email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Board, unless posting is in the course of business duties*")

APPENDIX B
UNACCEPTABLE USES

Unacceptable uses of the computer network include, but are not limited to, the following:

1. Unauthorised release of information*:*

- giving out personal information about another person, including home address and phone number,
- Providing information about, or lists of employees to outside parties;
- Providing confidential information about the Board or its operations to outside parties.

2. ***Unauthorised personal use:***

- use of the for personal business or commercial or for-profit purposes;
- product advertisement or political lobbying including the sending of "junk mail" or other advertising material;
- downloading entertainment software or other files not related to objectives of the Board for transfer to a user's home computer, personal computer, or other media.(including freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the Board);

3. ***Misuse of Passwords:***

- revealing a password to any unauthorized person;
- writing down a password;
- attempting to discover another user's password;
- allowing use of employee's account by an unauthorized party including family and other household members when work is being done at home.
- circumventing user authentication or security of any host, network or account;
- misrepresenting other users on the network

4. Unauthorized use or modification of equipment or software:

- intentionally modifying hardware, software, files, mailbox, web page other data, or passwords belonging to other users;
- unauthorized installation of any software, including shareware and freeware;
- malicious use of the computer network to develop programs that harass other users or infiltrate a computer or computing network and/or damage the software components of a computer or computing network;
- any activity that uses significant bandwidth unless specifically authorized by the network administrator (eg. establishing connections to live communications, including voice and/or video, streaming radio, itimes, voice communications and other similar uses);
- making unauthorized entry to other computational, information, or communications devices or resources

- introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- effecting security breaches or disruptions of network communication. including but 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.

5. Improper, objectionable or unethical actions:

- creating or circulating hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviours;
- using the computer network services in a malicious, threatening, or obscene manner;
- use of the computer network to access or process pornographic material or other inappropriate text files (as determined by the network administrator or building administrator), or files dangerous to the integrity of the local area network;
- use of profanity, obscenity, racist terms, or other language that may be offensive to another user;
- sending forged or anonymous e-mail or postings;
- any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages;
- using Board resources for any activities that are offensive or perceived to be offensive to others.

6. Misuse of Copyright:

- downloading, copying, or otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner, except when permitted for educational purposes;
- installation or distribution of products that are not appropriately licensed for use by the Board.

7. Frivolous uses

- transmission of jokes;
- playing games;
- instant messaging.