Acceptable use of Computer Network

Office Staff

Purpose

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.

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

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.

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

1. purposes related to the specific functions of each employee's job or purpose required to assist employees in carrying out the duties of their employment;
2. reasonable private purposes which are consistent with the procedure; and
3. those uses set out in **Acceptable Uses** to this procedure.

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

1. any use by an employee that significantly interferes with the duties of employment;
2. any use by an employee that exposes the Board to significant cost or risk of liability; and
3. those uses set out in **AP480 Appendix-Unacceptable Uses** to this policy.

The rules set out in this procedure 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.

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, or immediate supervisor.

Monitoring

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.

The Board keeps and may monitor logs of usage of equipment which may reveal information such as:

- 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

Except as otherwise provided for in this policy the Board:

1. will not engage in real-time surveillance of internet or equipment usage; and
2. will not disclose any of the logged, or otherwise collected information to a third party except under compulsion of law.

Surveillance and disclosure by the Board may take place in the following circumstances:

1. in the case of a specific allegation of misconduct, the Director or designate or Superintendent of Human Resources authorize accessing of such information when investigating the allegation;
2. when the IT Support section cannot avoid accessing such information whilst fixing a problem.

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

Copy right

The software and firmware is licenced by the Board and shall not be copied, removed erased or in anyway alter the original installation of said software and firmware

Security

1. Employees shall not attempt to gain unauthorized 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.
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.

User Names and Passwords

1. Employees who require computer network access in order to perform the functions of their employment will be assigned
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

Hardware and software is purchased by the Computer Systems administrator. Any software that is required and is not initially provided on the installed workstation must be requested from the Computer Systems administrator to assure compatibility to the required task and the computer system.

Remote Access

Remote Access is determined on a case by case basis. Requests are given to Computer Systems Administrator by the immediate supervisor of the employee.

Enforcement

1. Violation of this Administrative Procedure may lead to immediate denial of access to the computer network or to a particular device or service.
2. Any employee found to have violated this Administrative Procedure may be subject to disciplinary action, up to and including termination of employment.
3. Legal implications (if someone commits a crime using the Board equipment).

Also see: AP 480 Appendix; Unacceptable Use of Computer Network