Appendix B

Information Security and Acceptable Use Policy

For end-users of information stored in the Ministry of Education systems.

1. Introduction

In order to assist end-users with understanding their responsibilities in accessing information stored in ministry systems and to provide direction around appropriate use, the ministry has implemented a protection of privacy and access to information policy.

The primary goals of this policy are to protect the personal information stored as well as the confidentiality, integrity and availability of the ministry's information technology assets (software and information stored on the systems):

Confidentiality	Refers to ensuring that information is accessible only to those individuals who are explicitly authorized to view it.
Integrity	Refers to ensuring that information is protected from unauthorized or inadvertent modification so that it remains accurate and complete and can therefore be relied upon for use in making educational business decisions.
Availability	Refers to ensuring that systems and the information that they contain are available when the end-user requires them.

In order for a security policy to be successful, all end-users must be aware of potential security threats, their responsibilities in regard to those threats, and rules related to the acceptable use of the information.

2. End-User Responsibilities

Security breaches have a small number of root causes. They include: stolen or weak (easily guessed) passwords, physical access to unattended workstations, physical access to information held outside the system (printed output, digital media) and computer viruses. Fortunately, there are things that end-users can do to mitigate these threats:

2.1 Protect your password.

- never share your password with another individual;
- do not write your password down;
- do not use passwords that refer to personal data (i.e. children's names or your birth date);
- do not use passwords that contain dictionary words;
- do not type your password in when someone is looking over your shoulder; and,
- if your password has been inadvertently disclosed, change it immediately.

2.2 Protect your workstation.

- Never leave your work area without logging off or locking your workstation.

2.3 Protect your programs and information from viruses.

- Users should avoid clicking on any suspicious links or email attachments.

2.4 Protect information that is held outside of the system.
- store any digital media containing sensitive information in a physically secure location when not in use;
- ensure that paper, if required, containing sensitive information is protected from unauthorized access; and,
- ensure that sensitive information is appropriately destroyed when no longer required.

2.5 Immediately report to the ministry all security-related incidents, including:
- violations of Security or Acceptable Use Policy (all suspicious activity should be reported);
- security flaws or weaknesses that you discover while accessing ministry systems; and,
- computer virus infections.

3. Director of Education Responsibilities

Dormant network accounts are a primary target of hackers and disgruntled employees. This threat can be minimized by promptly disabling all accounts which are no longer required.

3.1 For schools using ministry applications, the Director is responsible for promptly notifying the Security Administrator when an individual is terminated, moves to another school, or when that individual will be taking a leave (definite/indefinite) of greater than 60 calendar days.

3.2 For schools with an electronic interface with ministry systems, the Director must ensure that policy and procedures are in place to ensure 1) that accounts are disabled when no longer needed, and 2) security audit reports can be produced by their system.

4. Acceptable Use

End-users are expected to exercise good judgement in determining whether or not a particular activity is an acceptable use of ministry systems.

4.1 ***Acceptable use includes***:
- enrolling students attending your school;
- withdrawing students from your school;
- updating student information; and,
- printing or producing reports as required by an authorized entity.

4.2 ***Unacceptable use includes***:
- disclosing confidential information to individuals or organizations with no written or formal authority to possess that information;
- viewing or distributing data files belonging to another user unless specifically authorized to do so, regardless of whether a security weakness in the system might permit this (the ability to access information does not implicitly grant permission to view that information);
- reading another user's information files from a display terminal, as printed output or from a data storage device without that user's explicit permission;
- requesting or attempting to learn another individual's password;
- using or attempting to use another individual's account;
- using department computer systems as a conduit for unauthorized access attempts on remote computer systems;

- attempting to intercept, block, de-crypt or eavesdrop on any electronic message addressed to another individual; and,
- developing, downloading or using programs that attempt to bypass security mechanisms or uncover security weaknesses.

5. Monitoring and Enforcement

The Ministry of Education has the ability to monitor individual system usage through the use of logs and other tracking tools. In the interest of enforcing security and acceptable use policies, it reserves the right to employ any tool or activity necessary for monitoring, auditing and, where necessary, controlling end-users' access to the system.

6. Communication of Policy

This "Acceptable Use Policy" is intended to make end-users aware of their responsibilities in accessing information stored in ministry systems. This document should be made available to all employees of school divisions, the Conseil des écoles fransaskoises or First Nations schools who have been assigned user access. There is an expectation that the content of the policy will be reviewed with end-users on a regular basis (i.e., twice per year).