RESPONSIBLE USE AND SECURITY OF INFORMATION TECHNOLOGIES

Background:

The Division is committed to protecting the integrity of its Information Technology (IT) assets, network and electronic information. The Division provides access to a secure, equitable computing environment for staff and students while recognizing the need to balance risk and responsible use of technology.

Definitions:

Division Network:
includes all wired and wireless computer networks in the Division.

Information Technology Asset (IT Asset):
includes all Division-owned equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. This includes assets such as servers, computers, laptops, mobile devices, tablets, wireless networks, printers, copiers, fax machines, scanners, displays, projectors, audio systems, monitors, firewalls, routers, switches, memory devices and software. Although peripherals and consumables—for example keyboards, mice, web cameras and chargers—form part of the asset, they're not subject to asset control.

Security:
is the continual analysis and management of risks.

Users:
refers to all students, employees, contractors and volunteers using the Division network and IT assets.

Procedures:

1. The Division Information and Security Officer is responsible for the security of the network, including safeguarding computers through the use of the firewall to protect staff and students from illegal or objectionable material and content.
2. Assets, equipment, network and software are the property of the Division. The Division Information and Security Officer retains the right to monitor and retrieve information as required.
3. The Division Information and Security Officer is responsible for the regular review of security requirements and related documentation.
4. Equipment and network are intended for educational purposes.
5. The Division Information and Security Officer is responsible for procuring all IT assets for the Division. Technology purchases are made through the IT Help Desk. All hardware device information is available through this link.

6. Any loss of equipment shall be reported as soon as possible to the Division Information and Security Officer.
    6.1. The Division Information and Security Officer will contact the Freedom of Information and Protection of Privacy (FOIP) Co-ordinator to assess risk and determine appropriate action.
7. Users shall exercise careful judgment when using the internet, intranet, email and IT assets.
8. Users shall be responsible to safeguard the network and report any infractions to administration.
9. Inappropriate use of IT assets and network may result in suspension, cancellation of access privileges, and/or disciplinary or legal action up to and including termination of employment.
10. All transmissions of personal information through technology shall be in compliance with Administrative Procedure 180: Freedom of Information and Protection of Privacy.
11. Responsible Technology Use
    11.1. Users shall adhere to Board Policy 19: Welcoming, Caring, Respectful, and Safe Working and Learning Environments when using IT assets and resources.
    11.2. Users shall adhere to Administrative Procedure 404: Employee Conduct.
    11.3. Users shall be required to review and sign the appropriate Student Responsible Technology Use (Appendix 140-B) or Staff, Contractor, Volunteer Responsible Technology Use Agreement (Form 140-2) in order to access the Division network.
        11.3.1. Annually at the start of each school year—or as needed throughout the school year for all families that enrol in the Division mid-year—parents/guardians shall acknowledge they've read and reviewed the Student Responsible Technology Use (Appendix 140-B) with their child.
    11.4. Users shall follow guidelines for password compliance and usage as outlined in the Information Technologies Manual (Appendix 140-A).
    11.5. Users shall follow guidelines for data storage as outlined in the Information Technologies Manual (Appendix 140-A).
    11.6. Users shall ensure confidential data is stored in a secure manner and encrypted when transported as per the Information Technologies Manual (Appendix 140-A).
    11.7. The Principal shall ensure the following:
        11.7.1. All current students have reviewed the Student Responsible Technology Use (Appendix 140-B) and parents/guardians have completed the corresponding acknowledgement each school year.
            11.7.1.1. The acknowledgement is first reviewed and signed upon enrolment in the Division.
            11.7.1.2. The acknowledgement is reviewed and signed by all returning students at the beginning of each school year.
        11.7.2. Current user acknowledgement shall not be stored in the student record.
12. The Associate Superintendent of Human Resources shall ensure the following:
    12.1. The Staff, Contractor, Volunteer Responsible Technology Use Agreement (Form 140-2) is completed and signed by all new staff.
    12.2. The agreement is stored in the personnel file.

12.3. Agreements will be reviewed by staff every three years or as identified by the Division Information and Security Officer.

12.4. The Principal or Director shall ensure contractors and volunteers who will be accessing the Division network complete the Staff, Contractor, Volunteer Responsible Technology Use Agreement (Form 140-2) and ensure the agreement is stored at the school or department site.

Reference:

Section 11, 31, 33, 52, 53, 197, 222 *Education Act*

Appendix 140-A: Information Technologies Manual
Appendix 140-B: Student Responsible Technology Use