INFORMATION AND INFORMATION TECHNOLOGY
- POLICY –

The Board of Education recognizes that information and information technology may change the way(s) that employees and students learn and work. This policy provides direction to staff and students on the appropriate use of information technology and the potential consequences of inappropriate use. This policy sets out the requirements that all employees must follow when accessing and managing district information, including confidential information.

Information technology includes all services and technologies used for creating, managing and transmitting information. Examples of services are the internet, information systems, applications, databases, voice and data networks, and electronic mail. Examples of technologies are smartboards, computers, laptops, tablets, printers, fax machines, telephones, USB drives, smartphones and other mobile devices.

The Board expects staff to use appropriate information technology to support and enrich the curriculum and to provide guidance and instruction to students in the appropriate use of information technology.

The Board acknowledges that the nature of information technology and the manner in which information is accessed makes it impractical to monitor all use at all times. The burden of responsibility therefore lies with individual users to ensure that they make appropriate use of information technology consistent with the intent of this policy.

- REGULATION -

1.0 DEFINITIONS

1.1 **Confidential Information:** a category of **District Information** with confidentiality requirements. It includes, but is not limited to:

- Planning information (for example, information about a proposed administrative plan that has not yet been implemented or made public);
- Third party business information, where its disclosure could harm the third party;
- Personal Information; and
- Legal advice or law enforcement information.

1.2 **Device:** an information technology resource that can connect (wired, wireless or cellular) to the district network, including but not limited to computers, laptops, tablets, smartphones, and cellphones.

1.3 **Employee:** an individual working for the school district, including a **Service Provider** or volunteer.

1.4 **District Information:** all recorded information relating to district business, regardless of format, that is received, created, deposited or held by any school, department or work site, reporting or responsible to the school district.

1.5 **Information Incident:** a single or a series of unwanted or unexpected events that threaten privacy or information security, including a privacy breach or the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the owner of that information.

1.6 **Information Technology Resources:** information and communication technologies that include, but are not limited to: information systems, **Devices,** and the district electronic network.

1.7 **Least Privilege:** a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use.

1.8 **Need-to-know**: a principle where access to information is restricted to authorized employees that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

1.9 **Personal Information:** recorded information about an identifiable individual other than business contact information.

1.10 **Portable Storage Device:** a portable (or removable) device that is primarily designed to store electronic information, for example an external hard drive or a USB flash drive.

1.11 **Protected District System:** a computer system in a work site that has met the approved security requirements for the storage of **Confidential Information** (for example, network drives). This does not include the hard drives of computers, laptops, tablets, smartphones or other **Devices.**

1.12 **Record:** anything that is recorded or stored by graphic, electronic, mechanical or other means, including books, documents, maps, drawings, photographs, letters, vouchers, and papers.

1.13 **Service Provider:** a person retained under contract to perform services for the school district.

2.0 ROLES AND RESPONSIBILITIES

2.1 Senior Administration - The Superintendent and Secretary Treasurer are responsible for issuing directives and guidelines on the appropriate use of district information technology and district information.

2.2 Supervisors

2.2.1 Supervisors are responsible for ensuring that employees are made aware of their responsibilities concerning the appropriate use of district information and district information technology:

- At the commencement of their employment;
- When a significant change occurs respecting their access to, or authorized use of, district information or their use of district information technology, including the issuance a new device;
- When a new or updated version of this policy is issued; and
- Annually for employees that have access to a significant amount of confidential information.

2.2.2 Supervisors must authorize an employee's access to district information based on the principles of "Need-to-know" and "Least Privilege". Specifically, an employee should have access to the least amount of confidential information that is necessary to perform their duties.

2.2.3 Supervisors must review an employee's level of access to confidential information at least once per year to ensure that their access level remains necessary and appropriate for the performance of their duties.

2.2.4 Supervisors are responsible for ensuring that employees receive the level of training (including privacy, security and records management training) necessary to perform their duties. In addition, supervisors are responsible for approving the downloading of applications and software by employees. This includes exercising due diligence to ensure that applications and software that are approved for download meet the requirements of this policy.

Supervisors must ensure that employees:

- Understand what confidential information is and the policies and procedures that must be followed when accessing and managing confidential information;
- Have received training appropriate to their position respecting the management of confidential information (including privacy, security and records management training) and what to do if an information incident occurs; and
- Have received approval for working outside the workplace with confidential information and for ensuring compliance with this policy.

2.2.5 Supervisors must report any suspected or actual information security concerns to the Secretary Treasurer and take actions necessary to protect the confidentiality, integrity and availability of information.

2.3. Employees

2.3.1 Employees are responsible for complying with this policy and for seeking direction from their supervisor(s) if they have questions regarding this policy. Employees must comply with the Standards of Conduct for Employees (PM 4-42) when:

- Collecting, accessing, using, disclosing or disposing of district information;
- Using information technology, whether that use is directly related to their employment duties or not; and
- Accessing third party hosted sites (e.g. Facebook and Twitter) in a manner that could be perceived as representing the district.

2.3.2 Employees must collect, access, use, disclose and dispose of district information in accordance with policy and law. For example, disposal of information must be done in accordance with approved records schedules, and collection, access, use and disclosure of personal information must be in accordance with the Freedom of Information and Protection of Privacy Act and relevant board policies.

2.3.3 Employees must prevent unauthorized disclosure, use, loss or destruction of district information and protect credentials, e.g., personal identifiers, passwords, access cards, keys and tokens. Employees must ensure that their use of information is lawful, does not interfere with their duties and responsibilities, and does not compromise the privacy and security of district information.

Employees are not permitted to:

- Install unauthorized software on district owned devices;
- Distribute or store inappropriate material; or
- Store district information on unauthorized devices.

Employees should be aware that the district has the right to monitor information and technology resource usage. Inappropriate use of information or information technology may result in disciplinary action or contract termination.

2.3.4 Special Responsibilities of Educators. Educators are required to:

- Provide developmentally appropriate guidance and instruction to students in the proper use of information and information technology, prior to giving students access to the internet, either as individual users or as members of a class or group;
- Apply policy 2-290 Selection of Learning Resources when guiding students to internet-based learning resources; and
- Monitor student use of information technology on a regular basis to ensure that the expectations of Board and school policies are being followed.

2.4 Students

2.4.1 Students are expected to use school district networks, computers and devices in a responsible manner. Appropriate use of information technology resources, consistent with Board and school policies, is expected.

2.4.2 Students are permitted to use information technology to conduct research, gather information for use at school and to communicate with others in educationally beneficial ways.

2.4.3 Students are expected to use information technology resources only after they have submitted written proof of parental approval, and only under the appropriate supervision and guidance of their teachers.

3.0 GENERAL REQUIREMENTS FOR USE OF INFORMATION AND INFORMATION TECHNOLOGY

3.1. Information Security

3.1.1 The usage and performance of systems are routinely monitored to protect against risks and to detect incidents or vulnerabilities.

3.1.2 Protection of information resources is the primary goal of information security. This includes practicing safe computing behaviours to reduce the overall occurrence of theft, loss, or misuse of information resources.

3.1.3 A breach in information security or loss of information assets can have serious consequences, depending on the sensitivity and value of the information and the extent of the breach. The consequences may include:

- Disclosure of personal information;
- Interruption in service delivery;
- Financial losses related to correcting the situation;
- Threats to public safety or individuals' health and well-being;
- Legal actions; and
- Erosion of the public trust in the Board.

Many factors amplify these concerns:

- Unauthorized use or disclosure of personal information is a security and/or privacy breach.
- Personnel who access inappropriate internet sites (e.g., offensive or illegal material, on-line gaming, dating) can bring public education into disrepute, harm the Board's reputation or introduce malicious code into the district's systems.
- Installation of unauthorized software can introduce security risks or impose unacceptable terms and conditions.
- Unauthorized use of copyrighted material is an infringement of intellectual property rights.

- The use of information technology for non-work related internet browsing can result in loss of productivity and introduce risks to the district's systems.
- Use of unauthorized devices and media can result in privacy and security breaches (e.g., unprotected USB devices).
- Personnel may incorrectly assume an expectation of privacy for personal, non-work related activity on information systems. All information stored or transmitted on the district's systems may be monitored, inspected or investigated.
- When a security or privacy breach occurs additional costs to Board are incurred.

Education and awareness are essential to promote an understanding of the importance of information security.

3.2 Use of District Networks

3.2.1 Network administrators are expected to monitor use of the network regularly, to maintain system integrity and to insure that users are using the system responsibly.

3.2.2 All information stored on school district computers and devices is the property of the school district. Due to limited storage capacity or technical necessity, files may be purged by the network administrator at any time without prior notification.

3.2.3 The Board reserves the right to review any material stored on school district computers and devices and will edit or remove any material which the Board believes may be unlawful, obscene, abusive, or otherwise.

3.2.4 All information services and features contained on the network are intended for private use. Any commercial or unauthorized use of those services and features is expressly forbidden.

3.3 Activities Not Permitted - When using information technology resources, the following activities are not permitted:

- Sending or displaying offensive messages or pictures;
- Using obscene language;
- Harassing, insulting or attacking others;
- Damaging computers, other devices or components of computer networks;
- Violating copyright laws;
- Using others' passwords;
- Trespassing into folders, work or files of others;
- Installing malware, viruses, root-kits, key loggers or other unauthorized software;
- Removing or upgrading software installed by IT staff without approval;
- Using the network for commercial purposes;
- Using information technology resources in a way that is not consistent with Board policies or an educational program as defined in the School Act.

3.4 Sanctions - Failure to adhere to this policy may result in:

- Loss of access or restricted access to Information Technology Resources;
- Disciplinary action;
- Involvement of law enforcement or other agencies.

4.0 COLLECTION, ACCESS, USE, DISCLOSURE, STORAGE AND DISPOSAL OF DISTRICT INFORMATION

4.1 Employees are responsible for ensuring that the confidential information they are working with is protected. This includes, but is not limited to:

- Storing confidential information in Protected District Systems;
- Physically securing confidential information in their workspace (e.g. locked drawers or cabinets);
- Storing confidential information using encryption;
- Only disclosing confidential information to authorized individuals in a secure manner according to approved processes (e.g. portable storage devices should only be used in extenuating circumstances when more secure methods are not available and must be encrypted); and
- Limiting the amount of confidential information, particularly personal information (which is subject to legal restrictions), that is disclosed through email.

4.2 Employees may work outside the workplace with confidential information provided that they have their supervisor's approval and comply with all the provisions of this policy. In addition, employees must:

- Protect the information, particularly when working in a public environment (for example, ensuring that information is not viewable or accessible by others);
- Limit the amount of printed materials that are used outside of the workplace (district computers are more secure because they are protected with district security features); and
- Ensure the information stored on any device outside the worksite is encrypted.

4.3 Employees and supervisors must immediately report any suspected or actual Information Incident (including a privacy breach) to the Secretary Treasurer.

5.0 USE AND DISPOSAL OF DISTRICT INFORMATION TECHNOLOGY

5.1 Reasonable personal use of district information technology by employees is permitted. Personal use is reasonable provided that it:

- Is limited during school hours and does not interfere with the employee's duties and responsibilities;
- Is lawful;
- Does not compromise the security of district information or district information technology; and
- Is not used for personal financial gain.

5.2 For privacy reasons and to reduce the cost of electronic storage for the district, employees must limit the amount they store on district systems related to personal use.

5.3 Employees must use their district email accounts when conducting district business. This includes while working outside of the workplace.

5.4 In extenuating circumstances, employees may use their personal email or other non-district email, as long as the following conditions are met:

- A copy of the email is sent to their district email account, ensuring that district information is stored in a Protected District System;
- The email is immediately deleted from their personal or non-district email account as soon as possible after dealing with the extenuating circumstance; and
- The amount of confidential information collected, accessed, used or disclosed is limited to the least amount necessary to deal with the extenuating circumstance.

5.5 To access district email accounts from a remote location, employees can use a browser to go to the Outlook Web App button on the district website home page.

5.6 Employees must not divulge, share or compromise their own or another employee's district authentication credentials (e.g., passwords, access cards, etc.).

5.7 Employees must report any lost or stolen district device.

5.8 Employees must follow the appropriate procedures when disposing of district devices. For further information, and to ensure proper disposal procedures are followed, please contact IT staff.

6.0 ACCESS TO AND USE OF APPLICATIONS AND SOFTWARE

6.1 Employees must have their supervisor's permission, and follow the established procedures, to download or use applications or software on any district computer or device.

6.2 Applications and software may present privacy or security concerns or could impose terms and conditions, such as indemnification clauses, that are unacceptable to the district.

6.3 Supervisors must not permit an employee to download or use applications or software that:

- Are prohibited by the district's IT staff;
- Present unacceptable privacy or security concerns; or
- Impose unacceptable terms and conditions.

7.0 MONITORING AND INVESTIGATIONS

7.1 Any collection, access, use, transmission, or disposal of district information or use of information technology, whether for personal reasons or not, may be audited, inspected, monitored and/or investigated to:

- Maintain, repair and manage IT Resources for the efficient operation of business systems;
- Meet legal requirements to produce information, including by engaging in e-discovery;
- Ensure accessibility of district IT Resources for the continuity of work processes;
- Improve business processes and manage productivity; and
- Ensure compliance with legislative and policy requirements, including the Standards of Conduct.

7.2 Allegations of inappropriate access, collection, use, disclosure, or disposal of district information or inappropriate use of district information technology will be investigated on a case-by-case basis. Investigations may include, but are not limited to, the search and/or seizure of devices.

7.3 Employees who inappropriately access, collect, use, disclose or dispose of district information or inappropriately use information technology may be subject to disciplinary action, including dismissal, cancellation of contract, and/or other legal remedies.