PROCEDURE SO-XXX

Acceptable Use of Information Technology

Board Received: _____ **Review Date:** _____

Purpose:
The purpose of this procedure is to ensure that staff and students are aware of the acceptable use of the Grand Erie District School Board's information technology network, hardware and software in order that they may take all reasonable precautions to maintain a safe, secure, positive and productive Information Technology environment for all users.

Definitions:
"Information Technology", is defined to include but is not limited to board owned:

- computers, data devices (e.g. phones, laptops, netbooks, & tablets) and hardware;
- servers and data storage devices;
- communication networks and associated devices;
- data;
- software;
- systems providing a service that are owned and/or maintained by a third party;
- peripherals;
- cloud based and subscribed apps and storage;
- blogs, websites and social media platforms.

"Grand Erie District School Board data", is defined to include;

- personal student, parent/guardian or staff information (including text, data, and media files), as well as materials considered to be of confidential nature with respect to school or board work.

"Communication Networks" is defined to include, but is not limited to:

- Board wireless and wired data networks;
- Connections to the Internet and Internet Service Providers (ISP);
- Remote connections i.e.. Virtual Private Network (VPN)

"Peripherals" is defined to include, but is not limited to:

- printers and copiers;
- robotics equipment;
- monitors, projectors, and interactive devices (i.e.. SMART boards, Assistive technology);
- portable data storage devices;
- input devices

"Users" is defined to include:

- students
- staff
- agencies of the Board
- partners of the Board
- volunteers
- parents/guardians
- guests

Process:

1.0 Responsibilities of the School Board

It is the responsibility of the Grand Erie District School Board to:

- Protect students and staff from misuse and abuse of information technology resources and services and will take all reasonable steps to ensure that they are used only for appropriate purposes
- Make all reasonable efforts to create and maintain a positive, productive, safe and secure Information Technology environment
- Maintain Information Technology resources and services
- Recognize the potential to support instruction and student learning as well as to support communication and collaboration across the system
- Maintain the right to monitor and access any and all files, documents and electronic communications and Grand Erie technology as well as use of the internet to ensure the integrity of the system and compliance with this procedure
- Grant network accounts to users to assist in fulfilling their employment duties and educational responsibilities
- Grant account access should there be a need for a supervisor to have access to that account, for example in the instance of an illness or investigation of inappropriate use, access will be granted through Information Technology Services in consultation with Human Resources and/or Director of Education. Access provided to the supervisor will be temporary and for the expressed purposes intended.

2.0 General Responsibilities of All Users

Take all reasonable measures and to ensure the safe, secure, ethical and appropriate use of Information Technology resources, as outlined herein, at all times

- All employees are expected to report the inappropriate use of the board's information technology resources in a manner that conflicts with the Board policies and procedures, or of the suspected loss or theft of board-owned computer property, or any unauthorized access, disclosure or inappropriate copying of confidential information
- Understand that a user's account is the property of the board and therefore that the user should have no reasonable expectation of privacy for any and all information stored or accessed through the board's network or on board devices
- Use and access board technology to the extent authorized by the board for the purpose of carrying out the mandate of the Board, regardless of the location of the equipment
- Use their own identity to access the board network and Internet resources
- Maintain privacy of their Grand Erie network credentials with others
- Exercise extreme caution when accessing emails from an external source
- Record passwords in a place that cannot be accessed by others
- Log out to protect their account when not in use
- Complete an on-line acceptance of the Acceptable Use of Information Technology declaration, annually
- Complete cyber security training during orientation and as determined necessary by the board
- Adhere to the expectations of Grand Erie's Social Media Guidelines
- Understand what restrictions and parameters exist under the Copyright Act including obtaining, transmitting and/or storing unauthorized copies of licensed and/or copyrighted material which may include, but is not limited to, software, music, video, or other such data
- Use the board's data network and Internet resources for personal use, provided that such use is reasonable in duration, does not interfere with the user's employment duties and responsibilities, does not result in increased cost to the board and is in compliance with this procedure. Personal use will occur outside of assigned work time.
- Share guest passwords with non-board employees for temporary access. The employee sharing the access code is responsible for the guest access
- Take reasonable steps to ensure that confidential information stored on Board network is not lost, stolen, modified, deleted or subject to unauthorized access, disclosure or copying, including:

- Be present when printing confidential information;
- Situate computer display terminals to prevent disclosure of confidential information;
- Use secure passwords for accessing the system;
- Access email and cloud resources on personal owned devices (laptops, tablets, or cellphones) only if the devices are password protected;
- Use certain forms of data protection and/or encryption depending on a user's role.
- Safely store computer equipment (i.e. laptops) when not in use or when transporting;
- Return all equipment and portable storage media to the Information Technology department for proper disposal or reuse
- Understand and apply the responsibilities under privacy legislation for how cloud-based applications are used to collect, use, share, and store/retain student personal information when considering the use of any external tools or applications
- Follow all applicable privacy legislation when leveraging external tools and applications
- Leverage School Messenger as the primary application for communicating personal information securely to parents/guardians;
- Contact ITS Help Desk if it is believed that user network credentials have been compromised and/or a data breach has occurred.

Failure to follow ***Acceptable Use of Information Technology Procedure (SO-XXX)*** without obtaining prior documented approval from the Manager of Information Technology Services or the Superintendent with Information Technology responsibility, or the Director, shall be construed as a deliberate and malicious act, the consequences of which will be carried out as per the Enforcement Section 8.0.

3.0 Responsibilities of Administrators, Managers and Supervisors

It is the responsibility of administrators, managers and supervisors to:

- Review and communicate the expectations of SOXXX annually with staff
- Ensure that staff complete an Acceptable Use of Computers and the Internet Online Declaration at the beginning of each school year
- Ensure that The Student Acceptable Use of Computers and the Internet Agreement (Appendix A) is signed and returned to the school at the beginning of each school year (administrators only)
- Use Multi-Factor Authentication on board issued devices to access board resources
- Co-operate fully with the board, local, provincial, or federal officials in any investigation concerning or relating to Information Technology.

4.0 'Responsibilities of Information Technology Services Staff

It is the responsibility of Information Technology Services Staff to:

- Provide and maintain a secure, safe, and productive Information Technology environment
- Enforce this procedure
- Inspect the contents of a user's device or other personal electronic data if:
  - directed by the user; or
  - required by law; or
  - required by the policies and procedures of the Grand Erie District School Board; or
  - at the direction of Human Resources and/or Director of Education in order to investigate complaints regarding inappropriate content which was intentionally sent or solicited, and is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or illegal material.
- Randomly scan data in order to expose instances of unauthorized software and/or data which must be reported to the site's Supervisor and/or deleted
- Refrain from sharing or communicating confidential information they come into contact with during their day to day activities. Any violation of this directive will be treated as a violation of this procedure

- Report violations of this procedure to their supervisor. In some cases, as required by law, staff may be expected to contact law enforcement agencies.
- Carry out activities which fall under the Unacceptable Activities defined in this procedure. These activities are to be undertaken by staff ONLY at the direction of Management in order to monitor and enforce this procedure, and in these specific cases will not be treated as violations. Such activities may include, but not be limited to:
    - Technical maintenance, repair and management
    - Produce information, including e-discovery, as per legal requirements
    - Restore deleted records/files
    - Conduct investigations involving employee use
    - Ensure continuity of work and continuous operations (i.e., employee is absent due to illness and work needs to be retrieved)
    - Improve Board processes and to manage productivity
    - Prevent misconduct and ensure compliance with the law by monitoring system activity, by conducting periodic audits to the system and by investigating potential misconduct.

5.0 Responsibilities of Students

Students should understand that use of Grand Erie Information Technology resources and services is a privilege. It is the responsibility of students to:

- Use information technology resources and services solely for educational purposes and comply with the directives contained in this procedure
- Review and complete the Student Acceptable Use of Computers and the Internet Agreement (Appendix A). The completed Student Acceptable use of Computers and Internet Agreement will be maintained by the school for the duration of the school year and then will be securely removed in June.

6.0 Responsibilities of Caregivers

In order that Caregivers are aware of their responsibilities under this procedure, they will be provided with the Student Acceptable Use of Computers and the Internet Agreement for signature annually. It is expected that caregivers will review this form with their child(ren). Caregivers should understand that use of Grand Erie Information Technology resources and services is a privilege. It is the responsibility of caregivers to:

- Review with their child(ren) and sign The Student Acceptable Use of Computers and the Internet Agreement (Appendix A).

7.0 Express Restrictions on Information Technology Use

The following unacceptable activities involving use of the Grand Erie's Information Technology resources are strictly prohibited. **Users must not:**

- Violate any local, provincial or federal statutes
- Store board data on any personally owned device or internet-based service (e.g. Gmail, Dropbox, etc.)
- Use electronic recording devices in schools and the workplace to record any interactions between two or more parties unless all parties explicitly consent
- Use the board's data network and Internet resources to violate a person's intellectual property, including by using the board's data network and Internet resources to engage in theft of software, music and movies
- Engage in personal use of the board's data network and Internet resources that interferes to any degree with the performance of their job responsibilities
- Use the board's data network and Internet resources for the purpose of carrying out a business enterprise without written authorization from the board, through the Superintendent of Business
- Respond to phishing emails where usernames and passwords are requested
- Use the board's data network and Internet resources for personal, financial or political causes
- Circumvent any security or control measures on the board network including the use of unauthorized Virtual Private Networks (VPN's).

- Use the board's data network and Internet resources for a purpose or in a manner that is inconsistent with the board's legitimate interests
- Intentionally delete emails with informational value to the detriment of legal and statutory Board operations
- Willfully collect, maintain or disclose personal information in contravention of the Municipal Freedom of Information and Protection of Privacy Act.
- Create, transmit, solicit or willingly accept, or store data which is defamatory or harassing towards any individual, contains obscene, indecent, lewd or lascivious material, contains profane language, panders to racism, sexism, any form of discrimination or other material which explicitly or implicitly refers to sexual conduct. including jokes, e-mails, music, videos, sounds, images, GIF's (graphics interchange format) or other electronic forms of information
- Violate any laws or participate in the commission or furtherance of any crime or other unlawful act
- Use Board computer equipment/resources to violate another person's intellectual property, including engaging in the theft of hardware/software, music and/or movies.
- Intentionally deface and/or damage Information Technology equipment
- Develop automations, scripts or viruses, designed to disrupt usage of Information Technology resources.
- Communicate information concerning passwords, identifying codes, personal identification numbers or other confidential information without the permission of its owner or the controlling authority of the school to which it belongs.

8.0 Enforcement

The enforcement of this procedure is the responsibility of all management. When the board suspects a violation of this procedure, it may restrict a user's access to the Board's computer equipment pending completion of an investigation. When the Board finds that a violation of this procedure has occurred, it may result in the imposition of one or more of the following:

- Restrictions on the use of specific Information Technology resources and services
- Suspension of access to all Information Technology resources and services
- Administration of the Progressive Discipline process found in Procedure HR119
- Disciplinary action up to and including expulsion (for students)
- Disciplinary action up to and including termination for employees
- Civil or criminal proceedings.

Use of technology is governed by all relevant federal and provincial laws, and Board's policies and procedures Activities that are in contradiction of this procedure will be reported to the appropriate level of supervision or management based on the user involved. In addition, the Board may report, or be required to report, suspected violations of the law to law enforcement and will cooperate with all local, national and international law enforcement agencies. The board is not responsible for steps taken by these agencies in the investigation and prosecution of public law.

References:

- Acceptable Use of Information Technology (SO-27)
- Grand Erie District School Board Code of Digital Citizenship (Appendix B)
- SO9 Cyberbullying (SO-9)
- SO11 Progressive Discipline and Promotion of Positive Student Behaviour (SO-11)
- SO12 Code of Conduct (SO-12)
- SO19 Privacy and Information Management (SO-19)
- SO24 Copyright – Fair Dealing Guidelines (SO-24)
- SO105 Privacy Breach Response (SO-105)
- HR103 Duties and Expectations of Teachers (HR-103)
- HR119 Progressive Discipline (HR-119)
- Grand Erie Social Media Guidelines
- *Municipal Freedom of Information and Privacy Protection Act*

Appendix A

Student Acceptable Use of Technology and the Internet Agreement

Background
Technology Resources, which include software, hardware, the Internet and other components, are an important ingredient to each student's education at our school.

Each student has the privilege of using the Technology Resources and must use them in an acceptable way.

Acceptable Use
As a general rule, students must use Technology Resources, including personal devices, in ways consistent with Provincial and Federal laws as well as consistent with the policies and procedures of the School and the School Board.

PROTECT
- I will not post information online that will put myself or others at risk.
- I will report any online attacks or inappropriate behaviour directed at myself or others.
- I will protect myself, my passwords and my resources.
- I will protect others by not forwarding inappropriate communications or materials.
- I will refrain from pirating or distributing digital resources that aren't free or don't belong to me.
- I will verify the accuracy of online information.

RESPECT
- I will give thoughtful consideration as to what personal information about my life, experiences and relationships I post.
- I will respect myself and others through my online actions and responses.
- I will not use electronic media to insult, bully, harass or stalk other people.
- I will not visit sites that are inappropriate.
- I will request permission to use online resources when necessary and cite all references to websites, books, media, etc.
- I will respect all equipment and all resources available to me.

School Name	
Student Name	

This is to confirm that I have read the Student Acceptable Use of Computers and the Internet Agreement and will abide by the rules and procedures as outlined.	
Signature of Student	Print Name
Signature of Caregiver Date	Print Name

Appendix B

Code of Digital Citizenship

CODE OF DIGITAL CITIZENSHIP

PROTECT + RESPECT

RESPONSIBLE ACTIONS IN A DIGITAL WORLD

PROTECT

- I will not post information online that will put myself or others at risk.
- I will report any online attacks or inappropriate behaviour directed at myself or others.
- I will protect myself, my passwords and my resources.
- I will protect others by not forwarding inappropriate communications or materials.
- I will refrain from pirating or distributing digital resources that aren't free or don't belong to me.
- I will verify the accuracy of online information.

RESPECT

- I will give thoughtful consideration as to what personal information about my life, experiences and relationships I post.
- I will respect myself and others through my online actions and responses.
- I will not use electronic media to insult, bully, harass or stalk other people.
- I will not visit sites that are inappropriate.
- I will request permission to use online resources when necessary and cite all references to websites, books, media, etc.
- I will respect all equipment and all resources available to me.

FOR INFORMATION ABOUT DIGITAL CITIZENSHIP, VISIT:

granderie.ca/digitalcitizenship