Acceptable Use of Information Technology

Board Received: March 26, 2018   **Review Date:**   April 2022

Policy Statement:

The Grand Erie District School Board believes that every user of Information Technology resources has a responsibility to follow all related Policies and take all reasonable measures and precautions to assist in ensuring the safe, secure, ethical and appropriate use of Information Technology resources at all times.

The Grand Erie District School Board will make all reasonable efforts, using the resources available, to create and maintain a positive, productive, safe and secure Information Technology environment.

Grand Erie District School Board has the right to monitor and may access any and all files, documents, and electronic communications on Grand Erie technology as well as the use of the Internet to ensure integrity of the system and compliance with this policy.

Grand Erie District School Board data is not to be stored on any personally owned devices. Staff are prohibited from using a personally owned device or computer to store board files or information. Staff must not use personal Internet based services (e.g. Gmail, Dropbox, etc.) to store board data files or information.

All measures that have been established to provide a safe, secure and productive environment, while protecting Grand Erie Information Technology resources against both internal and external threats, must not be altered, circumvented or otherwise disabled at any time.

Accountability:

1. Frequency of Reports – Annual
2. Criteria for Success   – Information Technology resources are used to enhance the delivery of curriculum and quality of education and to provide opportunities for collaboration, creativity, critical thinking, and communication.
   – Security, safety and productivity of Information Technology resources are maintained.
   – Criminal Code, Board Policy, and Code of Digital Citizenship are communicated and followed.
   – Monitoring is performed on an ongoing basis.

Procedures:

The Grand Erie District School Board believes that students and staff should have opportunities to:
- be both consumers and creators of information;
- collaborate and communicate with both local and global communities;
- develop knowledge and skills that will be useful through their lives.

The board, by providing and maintaining Information Technology resources and services, recognizes the potential to support instruction and student learning as well as to support communication and collaboration across the system. The board will make every effort to protect

students and staff from misuse and abuse of these services and will take reasonable steps to ensure that they are used only for appropriate purposes.

All equipment owned by the board is purchased for the purpose of carrying out the mandate of the Board, regardless of the location of the equipment. Board supported network accounts are granted to users to assist in fulfilling their employment duties and responsibilities. Authorized users may use the Grand Erie District School 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 complies with all components of this Policy. The expectation is that personal use will occur outside assigned work time.

It is important for all users to understand that a user's account is the property of the board and 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. Access provided to the supervisor will only be temporary and for the expressed purposes intended.

Reporting Expectations
- All employees are expected to report to their supervisor or the Manager of Information Technology knowledge they have of the use of the board's computer resources in a manner that conflicts with the Board policies, or of the suspected loss or theft of board-owned computer property, or any unauthorized access, disclosure or inappropriate copying of confidential information.

Network Access and Security
In addition to all related laws and Board policies, the following requirements exist:
- Users must only use and access board computer equipment as authorized and to the extent authorized by the board.
- Users must use their own identity to access the board network and Internet resources. Guest passwords may be shared with non-board employees for temporary access. The employee sharing the access code is responsible for the guest access.
- Users must not let anyone else use their identity to access the board data network and Internet resources.
- Users must not attempt to circumvent any security or control measures on the board network including the use of unauthorized Virtual Private Networks (VPN's).
- Users must refrain from recording passwords in a place that could be seen by others.
- Users must log out to protect their account from being accessed by others.

Express Restrictions on Use
- Users must not 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.
- Users must not create, view, transmit, store or copy information that is pornographic, obscene, threatening, defamatory or harassing (including against employer and other Grand Erie staff) or that expresses or implies an intention to discriminate.
- Employees must not 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.
- Users must not 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.
- Users must not use the board's data network and Internet resources for personal or political causes.

- Users must not 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.

1.0 Employee Duty to Protect Confidential Information

Employees have a responsibility to take reasonable steps to ensure that confidential information stored on Board network is not lost, stolen or subject to unauthorized access, disclosure or copying, including:
- Being present when printing confidential information;
- Situating computer display terminals to prevent disclosure of confidential information;
- Using secure passwords for accessing the system;
- Staff and Trustees may access email and cloud resources on personal owned devices (laptops, tablets, or cellphones) provided the devices are password protected;
- Depending on a user's role certain forms of data protection and/or encryption will be used.
- Safely storing computer equipment (i.e. laptops) when not in use or when transporting;
- Returning all equipment and portable storage media to the Information Technology department for proper disposal or reuse.
- Understanding 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.
- Depersonalizing student information that may be included when leveraging external tools or applications unless there is written consent to share student information (e.g. Using initials or non-identifying photos or videos).
- Leveraging School Messenger as the primary application for communicating personal information securely to parents. School Messenger allows for secure targeted personal information to get home in both written (text or email formats) and voice messages. Parent communication applications must allow users to opt out of messages.

This Policy is intended to ensure the safe, secure, ethical and appropriate use of these resources through education of users regarding what defines Acceptable Use of Grand Erie District School Board Information Technology resources. Failure to follow *Policy SO27 – Acceptable Use of Information Technology* 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 this policy section Enforcement found in Section 6.

2.0 Definitions:

In this Policy:

"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 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 ie. Virtual Private Network (VPN)

"Peripherals" is defined to include, but is not limited to:
- printers and copiers;
- robotics equipment;
- monitors, projectors, and interactive devices (ie. 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 and guardians
- trustees
- guests

3.0 Roles:

All users: Every user of Information Technology resources at the Grand Erie District School Board has a responsibility to follow this Policy and take all reasonable measures and to ensure the safe, secure, ethical and appropriate use of Information Technology resources, as outlined herein, at all times.

4.0 Additional Roles:

Students: Students should understand that use of Grand Erie Information Technology resources and services is a privilege. They are required to use these resources and services solely for educational purposes and comply with the directives contained in this Policy. Students are expected to treat these resources with respect. Students will review and sign The Student Acceptable Use of Computers and the Internet Agreement (Appendix A). The signed copies of The Student Acceptable use of Computers and Internet Agreement will reside in a binder in the office for the duration of the school year and then will be securely shredded in June.

Parents: Parents should understand that use of Grand Erie Information Technology resources and services is a privilege. Parents and their children will review and sign The Student Acceptable Use of Computers and the Internet Agreement (Appendix A).

Teachers: Teachers are responsible for reviewing with students The Student Acceptable Use of Computers and the Internet Agreement (Appendix A).

Principals and Managers: Principals and Managers are expected to review this Administrative Policy annually with staff and communicate these expectations to staff and students. They are

responsible for ensuring 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.

All Staff and Trustees: All Staff and Trustees will do an on-line acceptance of the Acceptable Use of Information Technology Policy on an annual basis. Principals and Managers will be responsible for tracking compliance of staff and the Director will be responsible for tracking the compliance of Trustees.

Management: All management will co-operate fully with the school board, local, provincial, or federal officials in any investigation concerning or relating to Information Technology.

Information Technology Services Staff: ITS staff are responsible for providing and maintaining a secure, safe, and productive Information Technology environment, and to enforce this Policy. This may include, but is not limited to, the activities defined below:

Email: All email and Internet communications sent and received by users are the property of the Grand Erie District School Board. Information Technology Services staff will not proactively inspect the contents of a user's email or other personal electronic data unless:

- directed by the user; or
- required by law; or
- required by the Policies of the Grand Erie District School Board; or
- at the direction of Senior Administration in order to investigate complaints regarding email which was intentionally sent or solicited, and is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or illegal material.

Data: Data stored within GEDSB Information Technology resources may be randomly scanned in order to expose instances of unauthorized software and/or data which must be reported to the site's Supervisor and/or deleted.

Information Technology Services staff may, from time to time, carry out activities which fall under the Unacceptable Activities defined in this Policy. These activities are to be undertaken by staff ONLY at the direction of Management in order to monitor and enforce this Policy, 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
- a legal requirement to produce information, including e-discovery
- restoring deleted records/files
- conducting an investigation involving employee use
- ensuring continuity of work and continuous operations (i.e. employee is absent due to illness and work needs to be retrieved)
- improving Board processes and to manage productivity
- preventing misconduct and ensuring compliance with the law including by monitoring system activity, by conducting periodic audits to the system and by investigating potential misconduct

Information Technology Services staff have privileged access to information and they are expected to report violations of this procedure to their supervisor. In some cases, as required by law, staff may be expected to contact law enforcement agencies.

Information Technology Services staff are strictly forbidden to share or communicate 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 Policy.

5.0 Unacceptable Activities:

The following Unacceptable Activities involving use of the Grand Erie District School Board's Information Technology resources are strictly prohibited:

Unacceptable Content: transmitting, soliciting or willingly accepting, or storing data which contains obscene, indecent, lewd or lascivious material, contains profane language, panders to racism, sexism, form of discrimination or other material which explicitly or implicitly refers to sexual conduct. This may include jokes, e-mails, music, videos, sounds, images, GIF's (graphics interchange format) or other electronic forms of information.

Hacking: attempting to gain unauthorized access to, or make unauthorized use of, electronic data and/or communications using the board's technology. This includes the introduction of unauthorized software to the Information Technology environment at the board.

Fraud*:* obscuring the true identity of a user while using Information Technology resources and services.

Copyright: obtaining, transmitting and/or storing unauthorized copies of licensed and/or copyrighted material which may include software, music, video, or other such data.

Unlawful Act: violating any laws or participating in the commission or furtherance of any crime or other unlawful act. Users must not use Board computer equipment/resources to violate another person's intellectual property, including engaging in the theft of hardware/software, music and/or movies.

Personal Use: use of the Board's Information Technology resources and services for unauthorized purposes including, but not limited to, political, financial or commercial gain, is strictly prohibited.

Personal Privacy: intentionally browsing, copying, deleting, modifying or seeking private information about another person unless specifically authorized. Access to public information about individuals is deemed acceptable.

Vandalism: intentional defacing and/or damage of Information Technology equipment.

Disrupting Usage: any activity, including the development of automatons, scripts or viruses, designed to disrupt usage of Information Technology resources.

Sharing Confidential Information of Another User: communicating 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.

Misrepresentation: Users must not share personal security information including passwords, logins, etc., with other users, nor are users allowed to log in to Information Technology resources using an account that has not been specifically assigned to them.

Unauthorized Access: All users are required to have been previously granted authorization to make use of Information Technology resources. This authorization may be granted explicitly to

an individual, or implicitly to a group. The failure to prevent unauthorized use of that resource does not relieve an individual of the responsibility of obtaining authorization prior to using the resource.

6.0 Enforcement:

ITS staff are responsible for providing and maintaining a secure, safe, and productive Information Technology environment. The enforcement of this Policy is the responsibility of all management.

When the board suspects a violation of this Policy, 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 Policy 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 student expulsion;
- disciplinary action up to and including employee termination;
- civil or criminal proceedings

Use of technology is governed by all relevant federal and provincial laws, and Board's policies and procedures (e.g. Copyright Act, Education Act, Acceptable Use Policy, codes of conduct and Progressive Discipline). Activities that are in contradiction of this Policy 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.

7.0 Related Policy, Procedures and Resources:
SO9 Cyberbullying
SO11 Progressive Discipline and Promotion of Positive Student Behaviour
SO12 Code of Conduct
SO19 Privacy and Information Management
HR103 Duties and Expectations of Teachers
HR119 Progressive Discipline
Grand Erie District School Board Code of Digital Citizenship (Appendix B)

Appendix A

Student Acceptable Use of Computers 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 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 Parent   Print Name
Date

* The signed copies of The Student Acceptable use of Computers and Internet Agreement will reside in a binder in the school office for the duration of the school year and then will be securely shredded in June.

Appendix B

Code of Digital Citizenship

Grand Erie District School Board
CODE OF DIGITAL CITIZENSHIP
"Protect and 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.

granderie.ca

CODE OF DIGITAL CITIZENSHIP