Section	PROGRAM	
Management Guideline	EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY	
Applicable Policy	EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY	602.2

Board Approved: February 25, 2025, February 19, 2020, May 23, 2012

Reviewed: February 4, 2025, November 12, 2024, February 19, 2020, May 1, 2012

Review by: December 2030

DEFINITIONS

"approved service provider" is an organization that provides educational or ancillary services to the Board, for example, a transportation consortium.

"employee" is a person who performs any work for, or supplies any services to, an employer for wages (excluding honoraria).

"information technology" refers to all forms of technology used to create, store, exchange, and use information in its various forms (data, audio, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).

"internet" means an electronic communications system connecting computers all over the world through which individual subscribers can interact and share information.

"spamming" refers to sending an annoying or unnecessary message to a large number of users.

"unlawful activity" see Appendix A

ADMINISTRATIVE PROCEDURES

1.0 Immediate supervisors will provide access to the Policy and Administrative Procedure at the work site and, upon request of an employee, will provide a personal copy of the policies and procedures.

2.0 Staff will be alerted to the existence of the Policy both by their immediate supervisor and Human Resource Services staff.

3.0 Human Resource Services will ensure all new staff acknowledge they have read and understood the Policy (and related guidelines) and will place a signed copy of the acknowledgement form in the employee's personnel file. An electronic acknowledgement of the Policy may also serve as the official record in lieu of a paper copy.

4.0 From time-to-time the IT Department, through the Director of Education or designate, will be authorized to allow access to a specific website that supports curriculum outcomes and may be outside the stated guidelines of the Policy.

5.0 Employees learning of misuse of board owned or managed Information Technology systems will notify their immediate supervisor.

6.0 The Board will, from time to time and without prior notice to the employee, access and/or monitor Information Technology systems owned or managed by the board. The necessity to access an employee or service provider's e-mail, internet, or voice mail or to disclose the contents may arise in a number of situations, including:

- to comply with disclosure requests or orders made pursuant to the Municipal Freedom of Information and Protection of Privacy Act; because of regular or special maintenance of the electronic information systems;
- when the Board has a business-related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable;
- in order to comply with obligations to disclose relevant information in the course of a legal proceeding or investigation; and
- when the Board has reason to believe that there has been a violation of this Policy or the Board's Code of Conduct.

7.0 Except with the prior approval of the appropriate supervisory officer, e-mail and internet are not intended to be used as a personal bulletin service. Solicitations, offers to buy and sell goods and services, and other personal messages to large groups on the internet are prohibited. (Examples at Appendix C)

8.0 Information Technology systems may not be used to store, distribute, post, download, or view any defamatory, abusive, obscene, profane, pornographic, sexually oriented, threatening, racially or ethnically offensive, sexist or illegal material.

9.0 Information Technology systems at a work site may not be used for any unlawful activity as outlined in Appendix A.

10.0 Information posted to the internet while conducting board business must comply with the Municipal Freedom of Information and Protection of Privacy Act, Board guidelines, and be consistent with the policies and Mission of the Board. (Examples at Appendix C)

11.0 School board business should be conducted using only school board assigned accounts and systems.

11.0 From time to time, employees will have in their possession electronic versions of student data. It is the employee's responsibility to safeguard that data under the Ontario Student Record Guidelines and, if applicable, the Municipal Freedom of Information and Protection of Privacy Act and/or the Ontario Health Information Protection Act. Employees who suspect that this data has been compromised shall notify their immediate supervisor. (Examples at Appendix C)

12.0 Information Technology systems will not be used to distribute confidential or proprietary information. Employees will not send confidential or proprietary information to recipients external to the Board, nor will they forward e-mails or other digital assets marked as confidential. Employees may, with the approval of a supervisory officer, exchange proprietary information with an Approved Service Provider

13.0 The Board's internet connection is a shared resource and, as such, employees shall make efforts to limit activities on the internet known to consume large amounts of bandwidth. These activities include streaming video, audio, and the transfer of large files/data. Where possible, video and audio used in the classroom should be captured/downloaded outside of school hours for later use. Streaming of video and audio for non-educational purposes is not allowed. (Examples at Appendix C)

14.0 Except with the prior approval of the appropriate supervisory officer, employees and service providers may not establish internet or external connections that could allow

unauthorized access to the Board's computer systems and information. These connections include (but are not limited to) the establishment of multi-computer file systems, ftp servers, e-mail servers, telnet, internet relay chat, wireless routers or remote control software.

15.0 This Policy will be interpreted in accordance with all relevant collective agreements.

16.0 Transmission of any unlicensed software, media, or any application having the purpose of damaging computer systems or files (e.g. computer viruses) is prohibited. All software and files downloaded must be systematically checked for viruses before loading on Board technology systems. Any malicious attempt to harm or destroy data of any person, computer, or network linked to the Board's Wide Area Network (WAN) is prohibited. (Examples at Appendix C)

17.0 Failure to comply with this Policy may result in the loss of access privileges, financial compensation to the Board, pursuance of criminal charges, and/or other disciplinary action up to and including discharge.

APPENDICES

Appendix A: Unlawful Activity
Appendix B: Form AT7 - Employee Acceptable Use of Technology Agreement
Appendix C: Management Guide Examples

References:

Policy 102: Mission Statement
Policy 607: Electronic Communications System
Policy 608: Computer Network Security
Policy 707: Employee Code of Conduct
The Education Act
The Libel and Slander Act, RSO 1990, Chapter L.12.
The Municipal Freedom of Information and Protection of Privacy Act

Appendix A

Unlawful Activity

For the purpose of this policy, **"unlawful activity"** is interpreted broadly and includes any criminal activity or other illegal activity.

The following are examples of **"unlawful activity"** for the purpose of the policy:

Child Pornography	Possessing, downloading or distributing any child pornography.
Intellectual Property	Infringing on another person's copyright, trade mark, trade secret of any other property without lawful permission.
Other Criminal Activity	Using electronic transmission as a means to commit criminal activity (examples include but are not limited to fraud, extortion, sale and/or purchase of restricted goods)
Defamatory Libel	A matter published without lawful justification or excuse, that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person. - *The Libel and Slander Act, RSO 1990, Chapter L.12.*
Disclosing or Gathering Personal Information	Disclosing personal information in a manner inconsistent with the *Municipal Freedom of Information and Protection of Privacy Act.*
Hacking and Other Crimes Related to Computer System	Examples include (but are not limited to): • gaining unauthorized access to a computer system • trying to defeat the security features of network connected devices • use of software and/or hardware designed to intercept, capture and/or decrypt passwords • intentionally spreading a computer virus • destroying or encrypting data without authorization and with the intent of making it inaccessible to others with a lawful need to access it. • interfering with other's lawful use of data and technology
Harassment	Sending electronic messages, without lawful authority, that causes people to fear for their safety or the safety of anyone known to them.
Hate Propaganda	Communicating messages that promote or incite hatred against an identifiable group that is likely to lead to a breach of the peace.
Interception of Private Communications or Electronic Mail (in transit)	Unlawfully intercepting someone's private communications or unlawfully intercepting someone's electronic mail.
Obscenity	Distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material.

Appendix B

Form AT7

EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY AGREEMENT

NEW EMPLOYEE TO THE BOARD

As a user of the Superior-Greenstone District School Board's (the Board's) Information Technology systems, I have read and hereby agree to comply with the Board's Policy 602.2, Employees' Acceptable Use of Technology and its related Management Guidelines 602.2.

EMPLOYEE NAME: _____
(Print Please)

EMPLOYEE SIGNATURE: _____ DATE:_____

WITNESS: _____ DATE:_____

Information Collection Authorization:

The personal information contained on this form has been collected under the authority of the Education Act R.S.O. 1980, C. 129, as amended and the Municipal Freedom of Information and Protection of Privacy Act, 1989.

This form will be handled with the strictest confidence. Questions about the collection of this information should be directed to the school principal or to the Superior-Greenstone District School Board's HR department and Freedom of Information/Protection of Privacy.

COPIES: (1) HR / (2) Employee (upon request)

TERMS AND CONDITIONS

It is the policy of the Superior-Greenstone District School Board to ensure that the Internet and Information Technology are used to support learning in a manner that is consistent with the Board mission statement, vision statement, and education goals.

1.0 Purpose of the Wide Area Network

- Use of the information technologies owned, operated, or administered by the Board must be used for the purpose of conducting Board business or the provision of an educational program.
- Use of the Board's Wide Area Network and its connection to the Internet for advertisement or monetary profit must have prior written Board approval.
- The Board will from time to time and without prior notice to the employee, access and/or monitor the Board's Electronic Information Systems

2.0 Network Etiquette and Citizenship

- The Board provides access to the internet for educational activities defined in the instructional plans of our teachers.
- Users will not post, publish, or display any defamatory, abusive, threatening, sexist, racially offensive, profane, obscene, sexually oriented, illegal and other material found to be offensive.
- The sending or storage of offensive messages from any source is prohibited.
- Users shall not copy information or software in violation of copyright laws.
- Software and resources downloaded will be used only under the terms and conditions specified by the owner or creator of those resources.
- Only staff who are authorized to download software or executable(.exe) programs may do so.
- It is prohibited for a user to post messages and attribute them to another user.
- Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

3.0 Vandalism

- Transmission of any software having the purpose of damaging computer systems and files (i.e. computer viruses) is prohibited. All software and files downloaded must be systematically checked for viruses before being placed on a school's network.
- Any malicious attempt to harm or destroy the data of any person, computer or network linked to the Board's Wide Area Network is prohibited and will result in financial compensation to the Board and/or the pursuance of criminal charges and/or other disciplinary action consistent with the School Code of Behaviour, Board Policy and/or legal authorities.
- Users will not attempt to gain unauthorized access to the Board's system or to any other computer system through the Board's system, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files. These actions are illegal, even if only for the purposes of browsing.

4.0 Security and Personal Safety

- Users may not share their passwords or accounts with others and must make all efforts to safeguard this information from unauthorized users.
- Users are advised to refrain from giving out personal information, such as their family name, email address, home address, school name, city, country or other information that could help someone locate or contact them in person.
- Users will not post identifying photos or videos.
- Users will not share intellectual property or digital assets of the board with outside organizations without the prior approval of the employee's supervisor.
- The Board reserves the right to block access to sites and to conduct regular checks of the system as deemed appropriate.
- An individual search will be conducted if there is reasonable cause to suspect that a user has violated the law or the school code of conduct. Personal files are discoverable under public records laws.

5.0 Inappropriate Material

- Interactive Internet gaming will not be accessed through the Board Internet Service without prior written authorisation
- Upon access to or receipt of material that is educationally inappropriate and contrary to the Board's Mission Statement, the employee shall immediately turn off the monitor and report the incident to their immediate supervisor.

Appendix C

Examples for Management Guidelines

The following are examples of how the Management Guidelines can affect your use of Information Technology at the work site:

No Solicitations *(7.0 Administrative Procedure)*	• No posting of advertisements on classified ad sites like Craig's List or Kijiji; • No bidding on, or selling items on eBay or similar sites, including the monitoring of bids; • No updating, visiting or posting to a website used for a personal enterprise; • Some activities are allowed with the approval of a Supervisory Officer and IT department.
Information Posted to the Internet *(10.0 Administrative Procedures)*	• When you access a website using school board assets or infrastructure, the source is identifiable as The Board and should be consistent with the mission and policies of the Board. Examples of "posting" include: ▪ Updating a WIKI; ▪ Contributing to a news group; ▪ Establishing a discussion thread in response to a blog post; ▪ Creating and/or contributing to a blog; ▪ Creating and/or updating a web site; ▪ Uploading a file to an FTP server or web site.
Safeguard Personal Data *(11.0 Administrative Procedures)*	• Exports of student data (TAB file, spreadsheet, marks etc.) must be on an encrypted USB key provided by the Board; • Personal Health Information must be encrypted; • If data is protected by password, the same care and attention must be given to the password as you would give to the data itself.
Internet *(13.0 Administrative Procedures)*	• No Internet Radio, or internet streams of terrestrial/satellite radio; • No audio or video streaming of sporting events; • Programs like RealPlayer or VDownloader should be used after school to download video to your hard drive rather than stream that content during the school day.
Unlicensed Software/Media *(16.0 Administrative Procedures)*	• No transmission/storage of music not legally owned by you; • No transmission/storage of video not legally owned by you; • No transmission/storage of software not legally owned by you; • No transmission or storage of software designed to defeat copy protection or licensing schemes, e.g. keygen, cracking or DVD decryption software.