Greater Essex County District School Board

Regulation: Digital Responsibility

Reference No: R-IT-03

1. Employees are expected to regularly use technology to enhance and enable their work.
2. Personal mobile and computing devices must not interfere with the learning / work environment. Personal devices should be turned off and stored away when not in use. It is permissible for staff to use personal devices if it directly supports teaching and learning (e.g. attendance, documenting student learning or student work)
3. The Board does not permit the use of Board Technology to create, distribute, or access any material which would not be considered suitable for any Authorized User. Inappropriate use of technology has the potential to cause significant damage to Board Technology, the reputation of the Board, and the trust relationship that the Board has with its students, their families and the public.
4. Access to Board Technology and Digital Content shall be by Authorized Users.
5. Authorized Users are not to use Board Technology for any Personal Commercial Enterprise.
6. Limited personal use of Board Technology (devices and/or network) is acceptable as long as it does not interfere with their own or others' work and/or learning and adheres to the requirements in this Regulation. Personal devices should be turned off and stored away when not in use.
7. Use of the Board Technology is a privilege. It does not limit the Board's ability to access information stored on Board Technology for a wide variety of legitimate reasons, including to engage in technical maintenance, repair and management, to meet a legal requirement to produce information, to ensure continuity of work (e.g., employee is sick or injured and work needs to be retrieved), to improve business processes and manage productivity and to prevent misconduct and ensure compliance with the law (including by monitoring system use, by conducting periodic audits of system use and by investigating potential misconduct).
8. Authorized Users should understand that (1) a password is what the Board uses to reliably identify who is using Board Technology (and how) and does not prevent the Board from accessing Board Technology and (2) that the Board can restore information that individuals delete. Authorized Users should also understand their use of Board Technology is not private. If Authorized Users need a private means of communication or a private means of computing they should use a personal computer or device and connect to the Internet through a commercial service provider.
9. The Board has final say for what purpose Board Technology is to be used.
10. Students and staff will be advised of this regulation, when they accept the digital responsibility notification when logging into the network. Parents / Guardians will be advised of elements of the digital responsibility regulation through the website and school handbooks.
11. When using technology, Authorized Users must:

11.1. Never impersonate, pose as another person, or falsify their identity in any way. Never use another individual's account unless is it is a necessary part of their job duties.

11.2. Never access or share any pornography, offensive or illegal material, unless it is required to uphold a Board Policy, Regulation, Administrative Procedure or Protocol.

11.3. Comply with the Copyright Act, and patent, trademark and criminal laws.

11.4. Follow established procedures for procuring Software and Digital Content not already licensed and/or installed by the Board.

11.5. Protect the identity and privacy of students and staff in accordance with their employment responsibilities or as directed by parents or guardians and authorized by administrators in accordance with the Board's Privacy of Information Policy P-HR-14 and Privacy of Information Regulation R-HR-14.

11.6. Refrain from accessing, using, modifying, copying, disclosing, and otherwise handling Digital Content (including the personal information of others) without authorization.

11.7. Never attempt to vandalize Board Technology, or harm, modify or destroy the Digital Content of other persons, the Board, or any agencies or other Networks that are connected to the Internet.

11.8. Comply with GECDSB Code of Conduct

11.9. Report without delay any problem, potential problem or vulnerability that may affect the security of Board Technology, any known or suspected incident of unauthorized access to or use of Board Technology and any known or suspect incident of unauthorized access to information stored on Board Technology:

- In the case of staff, to their Supervisor (see also paragraph 17.5)
- In the case of students, to their Teacher or support staff, who must then promptly report to their Principal or Vice Principal
- In the case of all other Authorized users, to the ITS Help Desk.

12. When using technology in relation to their role, employees are expected to:

12.1. Represent and conduct themselves, including when off duty, in accordance with the law and in accordance with the relevant standards of conduct expected of the employee group or profession as they would in any other environment where they represent the Board, their school or department.

12.2. Use a professional tone in all digital communications, and use speech and expression that is appropriate and not profane, disrespectful, slanderous, racist, sexist, libelous, insulting, threatening, hateful, unprofessional, discriminatory, harassing or bullying which are consistent with but not limited to Human Rights, the Board's Employee Standards of Conduct Policy P-HR-09, the Board's Employee Standards of Conduct Regulation R-HR-09, any applicable professional Standards of Practice, professional advisories, the Board's Workplace Violence Prevention Management Program and Workplace Harassment / Workplace Sexual Harassment Prevention Management Program.

12.3. Ensure any Digital Content deemed by the Board to be personal, confidential, or protected, on Board-owned or personal devices, either at the workplace or removed from the workplace, is adequately secured by password protection and/or encryption.

13. When using Board Electronic Communication Tools, Authorized Users should follow Board Best Practices, unless approved by the site/group owner, and are expected to:

    13.1. Only post or send charitable opportunity notices to sites provided by the Board e.g. the Water Cooler, or distribution lists authorized by their Supervisor (sending to individuals that they know personally is acceptable).

    13.2. Never send or post solicitation messages for the intent to provide or sell a product or service for personal business or corporate gain.

    13.3. Never send or post messages that promote or denigrate a political party or candidate.

14. When using Social Networking, Collaboration, Blogging, or Media sharing tools in relation to their role, Authorized Users are expected to:

    14.1. Use appropriate and respectful User Profile pictures, biographies, and other information to represent themselves.

    14.2. Maintain appropriate communications, only sharing information with others that they would willingly and appropriately share in a school or school-related setting or in the community.

15. When using Board-authorized Network Accounts, Authorized Users are expected to:

    15.1. Be personally responsible for all activity that occurs within their Network Accounts.

    15.2. Keep their passwords private and out of view of others and never share their passwords with another person, including Information Technology Services Department staff.

    15.3. Logoff or password-lock their Computers or Mobile Devices when not actively using them.

    Users of Board-authorized generic accounts are also responsible in the same way for those accounts.

16. Role and Responsibility of Supervisors

    Supervisors are responsible for supervising the work and conduct of their assigned staff including authorizing and overseeing their staff’s responsible use of technology and Digital Content. The following are examples of specific responsibilities of Supervisors:

    16.1. Ensure that assigned employees annually review and acknowledge understanding, acceptance of responsibilities, and compliance with this Regulation.

    16.2. Support assigned employees to use relevant technology and Digital Content in a responsible and appropriate manner.

    16.3. Model responsible use of technology and Digital Content.

    16.4. Address online behaviour that is harmful, unsafe and/or inappropriate.

    16.5. Report without delay any incidents described in paragraph 10.8 to the Superintendent of Information Technology or designate.

17. Role and Responsibility of Employees with Administrative Access to Computers or Information Systems

As determined by the Board, special administrative permissions to Board Technology, applications and Digital Content are granted to designated employees. These include, but are not limited to, Internet filter override accounts, network passwords and Supervisor-level access to report cards.

17.1. These special administrative permissions must not be shared with any other employee.

17.2. These employees are subject to a higher degree of due care and responsibility in protecting their Network Accounts, Board Technology, applications and all Digital Content in their purview.

17.3. These employees must only use their special access to undertake their work assigned in support of the Board's operation in their designated role.

17.4. They must never use their special administrative permissions to gain unauthorized access.

17.5. These employees must never share with any other person through any means, confidential information or Digital Content accessed or observed during the course of carrying out their assigned duties, except as may be reasonably required for training, demonstration, safety, legal or employment purposes.

17.6. These employees may not use their special administrative permissions for personal reasons or to further their own personal interests.

18. Role and Responsibility of Staff Supporting Students (teaching and non-teaching)

As part of their regular duties, staff are responsible for monitoring and supervising the work and conduct of students when using technology. The following are examples of responsibilities of staff:

18.1. Ensure the Digital Responsibility Agreement for Students is shared with, reviewed and acknowledged by students and parents/guardians annually.

18.2. Model responsible use of technology and Digital Content.

18.3. Address online behaviour that is harmful, unsafe and/or inappropriate using established student discipline procedures.

18.4. Confirm that parents/guardians have provided permission for their children before texts, pictures, videos, or audio recordings of students or their work are published on Digital Services.

18.5. Report without delay any incidents described in paragraph 10.8 to their Principal or Vice Principal.

19. Roles and responsibilities of students

19.1 Students are not required to supply personal mobile and / or computing devices for educational purposes as directed by an educator.

19.2 Students are encouraged to use, under the direction of their teacher(s), technology that is provided by their school or themselves to access and use a variety of Digital

Services provided by their school, the Board and external Internet sites. Students use technology to perform research, create Digital Content, to communicate, collaborate and share, and to complete their educational assignments.

19.3 Students use of personal mobile and computing devices are to meet the following criteria:

- For health and medical purposes;
- To support special education needs or;
- For educational purposes, as directed by an educator.

19.4 With permission from school staff or the people being photographed / recorded in advance, students can take photos, record audio and / or video in school buildings or during off site school sponsored events.

19.5 Student use of personal mobile and computing devices during instructional time, without appropriate permission, is grounds for discipline and / or confiscation of the device by school officials. Confiscated devices will be returned either to the student or parent / guardian after a reasonable period of time as determined by the school Principal. Unauthorized use of such devices may lead to disciplinary action, as outlined in the Progressive Discipline Regulation.

19.6 Student use of personal computing devices is acceptable during non-instructional time provided they pay attention to permission / consent clause above and follow the GECDSB Code of Conduct.

20. The Greater Essex County District School Board is not responsible for any loss, damage or theft to personal mobile or computing devices or data residing on those devices before, during or after it has been brought to school and/or connected to the GECDSB wireless guest network.

21. Regardless of the type of technology used or its ownership, and whether access to Board Technology is from within or from outside the Board, failure to comply with this Policy and Regulation may lead to corrective action, termination of network access privileges, and discipline according to applicable procedures.

Glossary

Authorized Users

Individuals are considered to be authorized users if:

- They are students of the Board, or
- They are employees of the Board, or
- They are members of agencies or organizations that have agreements with the Board, e.g. student teachers, auditors, etc.
- They are Trustees of the Board, or
- They are School Council Chairpersons, or
- They are members of the Greater Essex County Parent Involvement Committee (GECPIC) Executive, or
- They are guests of the Board and their limited access to the Internet only has been authorized by the Superintendent of Information Technology Services or delegate, or
- Their access to necessary computing resources has been authorized by a Superintendent in writing to the Superintendent of Information Technology Services or delegate.

Blog

A type of Digital Service for writing and posting articles or other Digital Content for the purpose of sharing and conversing with others; includes the ability to create a User Profile.

Board Technology

Includes but is not limited to all Board-provided computing equipment and devices, licensed software and computing services, Internet services used for educational purposes, network hardware, software and bandwidth.

Computer

A machine, typically in the form of a desktop, laptop, Network, tablet, or slate used by people to create, input, access, view, and share Digital Content.

Digital Content

Any data, files, pictures, or videos stored on or accessed with Computers and Mobile Devices.

Digital Service

A Network service such as interactive websites, electronic mail, online databases, filing systems, student information systems, business information systems, wikis, blogs, discussion boards, bookmarking and tagging, presentation sites, Digital Content storage, etc.

Discussion Forum or Board

A type of Digital Service designed to support online conversations in the form of primarily text based messages; often includes the ability to create a User Profile.

Internet

The global public Network outside of the Board’s control that includes all forms of Digital Services and Digital Content accessible for free or for a fee.

Intranet or Portal

A type of Digital Service provided by the Board to give employees a private and secure online space to work with Digital Content that requires a Network Account and password to gain access.

Mobile Device

A handheld or pocket-sized Computer or cell/smart phone that is usually connected to a Network and typically includes a display screen, usually with touch input or a small keyboard.

Network

A collection of Servers, Computers, and Mobile Devices connected together through various transmission media to facilitate Digital Services and digital communications among people.

Network Account

A credential consisting of a unique identity and a secret password that grans access to Network Resources, Digital Services, and Digital Content based on established access rights and permissions.

Network Resource

A Computer, Server or transmission bandwidth.

Personal Commercial Enterprise

The use of Board-owned technology for the gain of self or others in a profit-making business unrelated to the Board's educational goals.

Server

A specialized Computer used to deliver one or more Digital Services and to store Digital Content.

Social Network

A type of Digital Service that connects (e.g. "friend-ing", following) people to one another for the purpose of posting and sharing knowledge, information, and to encourage learning; often includes the ability to create a User Profile and to upload Digital Content for sharing purposes.

Social Bookmarking

A specific form of a Social Network to facilitate bookmarking (tracking) and sharing with others (publicly) of websites through the use of tags or keywords; includes the ability to create a User Profile and to follow other user's bookmarking activities.

Software or Apps (short for Applications)

The instructions and programming operating inside Computers, Servers, and Mobile Devices to enable them to perform the functions they are designed for.

Users

Persons authorized to access the Board and Internet Networks from Board and external sites.

Video, Audio, Photo, Image (media), and Presentation Sharing

Specific forms of Social Networks that support the uploading and sharing of Digital Content, specifically video, audio (podcast), photo, image, and presentation files; often includes the ability to create a User Profile.

Wiki

A type of Digital Service that supports collaborative creation and editing of webpages and Digital Content by Authorized Users; often includes the ability to create a User Profile.