Greater Essex County District School Board

Regulation: Network Security and Access

Reference No: R-IT-02

1. Network Security and Access

The purpose of the section of the Regulation is to define the standards, procedure and restrictions for connecting to the Greater Essex County District School Board's internal networks or related computing resources via hard wire.

This section of the Regulation applies to any equipment used to access GECDSB resources.

1.1. The Greater Essex County District School Board's Technology Council and Information Technology Services (ITS) department have the sole responsibility to recommend network technologies, implement network hardware and software, and secure access to this technology for GECDSB locations. The ITS department will:

1.1.1. Stay current on new networking technologies and recommend technology solutions that are reasonably secure and fit within the broader computing architecture.

1.1.2. Secure all approved networking implementations through the use of passwords and any other methods deemed necessary to ensure a safe computing architecture.

1.1.3. Develop, implement and maintain standard configurations for networking technologies.

1.1.4. Remove and dispose of any unauthorized communications technologies connected to the Board's network so that security standards are maintained according to the Board's Network Security Policy.

1.1.5. Take reasonable steps to prevent access to GECDSB computing resources by non-GECDSB-owned equipment via hard wire connection.

1.2. All users of networking technologies at the Greater Essex County District School Board also have a responsibility to support the security of the Board's computing resources. All users networking technologies at the Board will:

1.2.1. Not attempt to bypass any security measures put in place by the ITS department.

1.2.2. Refrain from connecting any unauthorized device such as a non-GECDSB owned laptop to the Board's network via hard wire.

1.2.3. Refrain from connecting any unauthorized device that may provide wireless access to the Board's network

1.2.4. Refrain from sharing or distributing any passwords provided for access to the Board's network.

1.2.5. Report any unauthorized networking implementations to the ITS Help Desk.

1.2.6. Report, without delay, any problem, potential problem, or vulnerability that may affect the security of the Board's networks and computing resources, any known or suspected incident of unauthorized access to or use of the Board's networks and computing resources and any known or suspect suspected incident of unauthorized access to information stored in the Board's networks and computing resources:

- In the case of staff, to their Supervisor.
- In the care 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.

1.2.7. Make no modifications of any kind to GECDSB-owned and installed networking hardware or software.

2. Use of the Board's networks and computing resources is a privilege. It does not limit the Board's ability to access information stored on its networks and computing resources 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 activity, by conducting periodic audits of system use and by investigating potential misconduct).

3. All users should understand that (1) a password is what the Board uses to reliably identify who is using its networks and computing resources and (2) that the Board can restore information that individuals delete. All users should also understand their use of the Board's networks and computing resources is not private. If 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.

4. Wireless Security and Access

The purpose of this section of the Regulation is to define the standards, procedures and restrictions for connecting to the Greater Essex County District School Board's internal networks or related computing resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- Wireless gateways at all Greater Essex County District School Board Premises

- External hosts via remote access technology (for example, using a router at home to connect to the GECDSB Virtual Private Network)
- Third-party wireless Internet service providers (also known as “hotspots”)

This section of the Regulation applies to any equipment used to access GECDSB resources; even if said equipment is not GECDSB-sanctioned, owned or supplied. For example, use of equipment owned by an employee and brought to a GECDSB location is included.

4.1. The Greater Essex County District School Board’s Information Technology Services (ITS) department has the sole responsibility to recommend wireless technologies, implement wireless hardware and software, and secure access to this technology for GECDSB locations. The ITS department will:

4.1.1. Stay current on new technologies involving wireless networking and connectivity and recommend technology solutions that are reasonable secure and fit within the broader network architecture.

4.1.2. Secure all approved wireless implementations through the use of passwords and any other method deemed necessary to ensure a safe computing environment.

4.1.3. Develop, implement and maintain standard configurations for wireless technologies to allow Greater Essex County District School Board users to roam seamlessly among Board sites.

4.1.4. Remove and dispose of any unauthorized wireless technologies connected to the Board’s Network Security Policy.

4.1.5. Provide limited access to GECDSB computing resources by non-GECDSB owned equipment, in particular to the internet which also permits access to GECDSB email. Take special note that this type of equipment is not supported by the ITS department, and any requests for support for it will be refused.

4.2 All users of wireless technologies at the Greater Essex County District School Board also have a responsibility to support the security of the Board’s computing resources. All users of wireless technologies at the Board will:

4.2.1 Not attempt to bypass any security measures put in place by the ITS department.
- Refrain from connecting any unauthorized device that may provide wireless access to the Board’s network.
- Refrain from sharing or distributing any passwords provided for access to the Board’s network.
- Report any unauthorized wireless implementations to the ITS Help Desk.

- Report without delay any problem, potential problem or vulnerability that may affect the security of the Board's networks and computing resources, any known or suspected incident of unauthorized access to or use of the Board's networks and computing resources and any known or suspect incident of unauthorized access to information stored on the Board's networks and computing resources:
  - In the case of staff, to their Supervisor
  - 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 user, to the ITS Help Desk.

Make no modifications of any kind to GECDSB-owned and installed wireless hardware or software. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations.

While the ITS department is not able to manage public or home wireless resources, all users of these resources will ensure that all components of their wireless connections remain as secure as their network access within a GECDSB location while using them to access computing resources at the Greater Essex County District School Board.

General access to GECDSB's computing resources through the Internet by employees at home is permitted. However, the employee using the Internet for recreational purposes through GECDSB networks are not to violate any of GECDSB's policies related to the use of computing technologies.

Users employing wireless access methods will, without exception, use secure remote access procedures. Users agree to never disclose their passwords to anyone, particularly to family members if work is conducted from home.

All remote computer equipment and devices used for GECDSB interests, whether personally or GECDSB-owned, must display reasonable physical security measures. Users are expected to secure their GECDSB-connected machines when they are physically at their machines, as well as when they step away. Computers will have whatever antivirus software is deemed acceptable by the ITS department. Antivirus signature files must be kept up to date.

Remote users using public hotspots for wireless Internet access must employ for their devices a GECDSB- approved personal firewall, VPN and any other security measure deemed necessary by the ITS department.

Any remote connection that is configured to access GECDSB computing resources must adhere to the authentication requirements of GECDSB's ITS department. In addition, all hardware security configurations (personal or GECDSB-owned) must be approved by GECDSB's ITS department.

All users will ensure that their computers are not connected to any other network while connected to GECDSB's network via remote access.

All connections that make use of wireless access must include a “timeout” system. Specifically, sessions will timeout after no more than 30 minutes of inactivity and will terminate after two hours of continuously inactive connection. Both timeouts will require the user to reconnect and re-authenticate in order re-enter the GECDSB network through a wireless connection.

All wireless access users acknowledge that accessing GECDSB owned printers from non-GECDSB owned equipment is not permitted. Any requests for support for this type of printing will be refused.

All wireless access users acknowledge that GECDSB is not responsible for any loss or damage to their non-GECDSB owned equipment or data residing on that equipment before, during or after its connection to the GECDSB network. Likewise, GECDSB is not responsible for any loss or damage to data or systems outside its network caused by non-GECDSB owned equipment before, during or after its connection to the GECDSB network.

All wireless access users acknowledge that their access and/or connection to the GECDSB network may be monitored to record dates, times, duration of access, data types/volumes, etc. in order to identify unusual patterns or other suspicious activity. As with in-house computing resources, this is done in order to identify accounts/computers that may have been compromised by external parties. Users should have no expectation of privacy in their use of the Board’s wireless network.

Violations of the Network Security Policy and associated Regulation may lead to disciplinary action.