Greater Essex County District School Board

Title: Network Security and Access
Category: Operational Procedure
Department: Information Technology
Responsibility: Superintendent of School Operations and Information Technology
Effective Date: May 20, 2009
Review Date: June 2, 2026
Next Review Year: 2031

Rationale

The Greater Essex County District School Board (GECDSB) recognizes that secure, reliable network access is essential to the delivery of teaching, learning, and administrative services. This Operational Procedure establishes the standards, procedures, and restrictions that apply to connecting to GECDSB internal networks and related computing resources — including hard-wired connections at Board sites, wireless connections at Board sites, and remote access from external locations.

The Board's Information Technology Services (ITS) department is responsible for recommending, implementing, securing, and maintaining all approved networking technologies. All authorized users share the responsibility of safeguarding the Board's networks and computing resources against unauthorized access, modification, or use.

Use of the Board's networks and computing resources is a privilege, not a right. The Board reserves the right to access, monitor, and audit information stored on or transmitted through its networks for legitimate purposes — including technical maintenance, repair and management, meeting legal requirements, ensuring continuity of work, improving business processes, managing productivity, and preventing or investigating misconduct. Users should have no expectation of privacy in their use of the Board's network.

This Operational Procedure applies to any equipment used to access GECDSB resources, regardless of whether the equipment is GECDSB-sanctioned, owned, or supplied. Equipment owned by an employee and brought to a GECDSB location is included.

Guiding Principles:

- Only ITS-approved networking technologies and configurations may be used to connect to the Board's network.
- All access to the Board's network must be authenticated and restricted based on need.
- All users are accountable for the security of credentials issued to them and for the equipment they use to connect.
- Suspected or confirmed network security incidents must be reported without delay through the appropriate channel.

- Failure to comply with this Operational Procedure may result in a loss of network access and/or disciplinary action.

Definitions

Authorized User
Any person granted permission to access the Board's networks or computing resources, including staff, students, trustees, contractors, and other individuals approved by the Superintendent of Information Technology Services or designate.

Board Network
The collection of servers, computers, switches, routers, wireless access points, and other transmission media operated by GECDSB to provide digital services and communications to authorized users.

Computing Resources
Hardware, software, applications, data, and services provided by or accessed through the Board's network, including but not limited to email, file storage, business and student information systems, and printing services.

Hard-Wired Connection
A physical, cabled connection (typically Ethernet) between a device and the Board's network.

Wireless Connection
A connection to the Board's network or to GECDSB computing resources made by any wireless means, including Board wireless gateways, third-party wireless Internet service providers ("hotspots"), and remote access through external networks.

Remote Access
Access to the Board's network or computing resources from a location outside Board premises, typically through a Board-approved Virtual Private Network (VPN) or equivalent secure remote access service.

ITS Help Desk
The first point of contact within Information Technology Services for reporting issues, requesting support, and reporting suspected security incidents related to the Board's network and computing resources.

Procedure

1. Hard-Wired Network Security and Access

This section defines the standards, procedures, and restrictions for connecting to the Board's internal networks or related computing resources via a hard-wired connection. It applies to any equipment used to access GECDSB resources.

1.1 ITS Department Responsibilities

The Information Technology Services department has sole responsibility to recommend network technologies, implement network hardware and software, and secure access to this technology for GECDSB locations. ITS will:

- Stay current on new networking technologies and recommend technology solutions that are reasonably secure and that fit within the broader computing architecture.
- Secure all approved networking implementations through the use of passwords, multi-factor authentication where appropriate, and any other methods deemed necessary to ensure a safe computing architecture.
- Develop, implement, and maintain standard configurations for networking technologies.
- Remove and dispose of any unauthorized communications technology connected to the Board's network so that security standards are maintained in accordance with the Board's network security requirements.
- Take reasonable steps to prevent access to GECDSB computing resources by non-GECDSB-owned equipment via hard-wired connection.

1.2 User Responsibilities

All users of networking technologies at GECDSB share responsibility for the security of the Board's computing resources. Users will:

- Not attempt to bypass any security measures put in place by the ITS department.
- Refrain from connecting any unauthorized device, including a non-GECDSB owned laptop, to the Board's network via hard-wired connection.
- Refrain from connecting any unauthorized device that may provide wireless access to the Board's network.
- Refrain from sharing or distributing any passwords or credentials provided for access to the Board's network.
- Report any unauthorized networking 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, and any known or suspected incident of unauthorized access to or use of the Board's networks, computing resources, or stored information.

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

2. Wireless Security and Access

This section defines the standards, procedures, and restrictions for connecting to the Board's internal networks or related computing resources via any wireless means. This includes, but is not limited to:

- Wireless gateways at all GECDSB premises.
- External hosts using remote access technology (for example, a router at home connecting to the GECDSB Virtual Private Network).
- Third-party wireless Internet service providers ("hotspots").

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

2.1 ITS Department Responsibilities

The Information Technology Services department has sole responsibility to recommend wireless technologies, implement wireless hardware and software, and secure access to this technology for GECDSB locations. ITS will:

- Stay current on new technologies involving wireless networking and connectivity and recommend technology solutions that are reasonably secure and that fit within the broader network architecture.
- Secure all approved wireless implementations through the use of passwords, multi-factor authentication where appropriate, and any other method deemed necessary to ensure a safe computing environment.
- Develop, implement, and maintain standard configurations for wireless technologies that allow GECDSB users to roam seamlessly among Board sites.
- Remove and dispose of any unauthorized wireless technologies connected to the Board's network.
- Provide limited access to GECDSB computing resources by non-GECDSB-owned equipment, in particular Internet access (which also permits access to GECDSB email). This type of equipment is not supported by the ITS department, and any requests for support for it will be refused.

2.2 User Responsibilities

All users of wireless technologies at GECDSB share responsibility for the security of the Board's computing resources. Users will:

- 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 or credentials provided for access to the Board's network.
- Report any unauthorized wireless implementations to the ITS Help Desk.
- Make no modifications of any kind to GECDSB-owned and installed wireless hardware or software, including but not limited to split tunneling, dual homing, and non-standard hardware or security configurations.

3. Remote and Off-Site Wireless Access

While the ITS department does not manage public or home wireless resources, all users of these resources will ensure that the components of their wireless connection remain as secure as their network access within a GECDSB location while they are using them to access GECDSB computing resources.

General access to GECDSB computing resources through the Internet from home is permitted. However, employees using the Internet for recreational purposes through GECDSB networks must not violate any GECDSB policies related to the use of computing technologies.

3.1 Required Practices for Remote and Wireless Users

- Users of wireless access methods must, without exception, use secure remote access procedures.
- Users must never disclose their passwords to anyone, including family members, when work is conducted from home.
- All remote computer equipment and devices used for GECDSB interests, whether personally owned or GECDSB-owned, must include reasonable physical security measures. Users are expected to secure their GECDSB-connected machines when they are physically at their machines and when they step away.
- Computers used to connect to GECDSB resources will use anti-malware/anti-virus software deemed acceptable by the ITS department, with signature files kept up to date.
- Any remote connection configured to access GECDSB computing resources must adhere to the authentication requirements of the ITS department. All hardware security configurations — personal or GECDSB-owned — must be approved by the ITS department.
- Users must ensure that their computers are not connected to any other network while connected to the GECDSB network through remote access.

3.2 Session Time-outs

All connections that make use of wireless access must include a time-out system. Sessions will time out after no more than 30 minutes of inactivity and will terminate after two hours of

continuous inactivity. Both time-outs require the user to reconnect and re-authenticate in order to re-enter the GECDSB network through a wireless connection.

3.3 Printing and Equipment Limitations

- Accessing GECDSB-owned printers from non-GECDSB-owned equipment is not permitted. Any requests for support for this type of printing will be refused.
- GECDSB is not responsible for any loss or damage to non-GECDSB-owned equipment or to 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.

4. Reporting Network Security Incidents

Any individual who becomes aware of, or reasonably suspects, a problem, vulnerability, or unauthorized access affecting the Board's networks or computing resources must report it without delay:

- Staff: report to their immediate supervisor.
- Students: report to their teacher or supervising staff member, who must promptly report the incident to the Principal or Vice-Principal.
- All other authorized users: report to the ITS Help Desk.

5. Monitoring, Privacy, and Use as a Privilege

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 technical maintenance, repair and management, meeting legal requirements to produce information, ensuring continuity of work (for example, when an employee is sick or injured and work needs to be retrieved), improving business processes, managing productivity, and preventing misconduct or ensuring compliance with the law (including by monitoring system activity, conducting periodic audits, and investigating potential misconduct).

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) the Board can restore information that individuals delete. Users should also understand that their use of the Board's networks and computing resources is not private. If a user needs a private means of communication or computing, they should use a personal computer or device and connect to the Internet through a commercial service provider.

Access to and connections through the GECDSB network may be monitored — recording dates, times, duration of access, data types, and volumes — in order to identify unusual patterns or other suspicious activity. As with in-house computing resources, this is done to identify accounts or 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.

6. Compliance and Discipline

Violations of this Operational Procedure may lead to corrective action, termination of network access privileges, and/or discipline in accordance with applicable Board procedures, collective agreements, and legislation.

7. Review and Continuous Improvement

This Operational Procedure will be reviewed periodically to ensure it remains effective, current, and aligned with best practices, legislative requirements, and related GECDSB policies. Reviews may be informed by audit findings, security incident reviews, changes in legislation, or emerging risks.

Reference

Board Documents:

- Cyber Security
- Digital Responsibility
- Privacy of Information
- Code of Conduct
- Records Management

Appendix

Not Applicable

Where a conflict exists between this Operational Procedure and another Board policy or procedure, the more stringent control or requirement shall apply.