



Network Security

Policy Code: 3240

Introduction

Technology equipment, including all computer networks, interactive classroom tools (projectors, interactive white boards, document cameras, etc.), and hardware, is the property of Franklin County Schools and is provided for educational and administrative purposes. For these reasons, the FCS Technology Department will work to ensure a secure and safe network, putting in place a variety of safeguards to help in that mission.

Authentication - Usernames and Passwords

Appropriate user security measures will be developed, implemented and maintained by the Technology Department. Unique usernames and passwords within the regulations and guidelines are established by the department, and follow the NCWISE username and password guidelines.

These regulations and guidelines will be provided to building level principals, school technology contacts and site based technology personnel.

Users should NEVER share a user id or password. Divulging usernames and passwords compromises security and could lead to dissemination of confidential employee or student information.

Employee Access to Data

Employees will be given access through assignment of user identifications and passwords to confidential data. A copy of the *Acceptable Use Agreement* form will be included in the Employee Handbook. All employees are responsible for maintaining confidentiality of employee or student information. It will be the responsibility of each employee to report to a supervisor if they suspect user identifications and passwords may be compromised. It will be the responsibility of each employee to report to a supervisor if they suspect criminal use of user identifications and passwords. It will be the responsibility of each employee's supervisor to report any compromises or criminal use of network identifications and passwords to the Superintendent's office.

Employees will save confidential data to their personal directory, located on a district server, rather than workstation hard-drives. Data saved to the network is protected by antivirus software and other electronic devices. Data saved to a network server is far more secure than data saved to a workstation.

Security Measures

The Technology Department office will implement and utilize a variety of security measures to prevent unauthorized access to and use of School System resources. These measures will include firewalls, filters, sniffers, and packet shapers. New tools, as they are developed and become

available, may be utilized to prevent security incidents and protect resources. No right of privacy exists in any communication on the network, materials stored, sent or received over the School System networks or computer systems. Monitoring of this material may occur to either ensure the security and operating performance of the information technology systems, or enforce the Board policies and compliance of applicable laws and regulations.

Confidentiality of Security Information and Security Measures

School System personnel will not weaken the security system and jeopardize the confidentiality of employee and student information by making the security infrastructure and security information public.

Privately owned computers, laptops, wireless access points, switches, mini-hubs, etc. will not be connected to the network, except in situations approved in advance by the FCS Technology Department.

Reporting of Information Technology Security Incidents

Employees are required to immediately report information regarding security incidents or breaches, which compromise the integrity of the systems or data, to their principal or supervisor. Principals and supervisors are required to report the incident to the District Technology Department who will investigate the incident and take appropriate action to eliminate any determined weakness in the security system. Chief Technology Officer is required to report any security breach to the Superintendent.

Technology Policies, Regulations, Standards and Guidelines

Upon approval by the Superintendent, the Chief Technology Officer may develop and adopt procedures, regulations, standards and guidelines to be followed by all employees and students regarding access and use of any technology related services and/or equipment that is not specifically addressed here.

Areas covered by these internal procedures, regulations, standards and guidelines may include hardware and software deployment, equipment maintenance and repair, disaster recovery of data and hardware, website management, and password guidelines. These policies, regulations, standards and guidelines will be published, after approval by the Superintendent, on the School System website in the Technology Department section.

Legal References: G.S. 147-33.111

Cross Reference: Acceptable Use Policy (Policy 3225), Standards of Expected Student Behavior (Policy 4310), Public Records (policy 5070), FCS Employee Handbook, FCS Student Code of Conduct

Adopted: 06/04/07

Revised: 08/08/11