



**POLICY 449 -- INFORMATION SECURITY**

**1. Objective**

The school district has an obligation to protect the privacy of its students and their families. Particularly, it must be in compliance with the Family Education Rights and Privacy Act, 1974. Likewise it has an obligation to ensure that while offering the necessary education and exposure to telecommunications skill and usage, appropriate steps are taken to protect children from risks inherent in the use of that technology.

Additionally, the school district, as an organization will continue to enhance its use of administrative computing to increase efficiency and the quality of services provided. However, it must take measures to protect against inappropriate access to, use of, or intrusion into its telecommunications network. It must protect its employees from risks related to inappropriate use of electronic communications. It must also take steps to protect the district from liability that may occur from the misuse of its electronic resources. These responsibilities include:

- Ensuring that student, employee and other confidential data is available only to authorized users
- Ensuring authorized users have access only to appropriate data and users are not able to access any other confidential or sensitive information.
- Ensure that services do not permit unauthorized access to data, systems or internal network
- Guaranteeing the authenticity and integrity of student and administrative data.
- Ensuring that the organizations IT infrastructure and systems meet the standards for data privacy and the architecture contains the necessary tools and techniques to protect sensitive data.

The purpose of this policy is to establish a high-level district-wide Information Security Policy. It also identifies some additional lower level technical policies, procedures and standards.

**2. Scope**

This security policy applies to information resources that are part of the education delivery environment, the student record keeping environment and the administrative environment of the District. It applies to resources and access to the computing / telecommunications environment in every District facility as well as remote access to the District electronic environment and information, equipment or

records that are owned by the District which may at any time be removed from or accessed from outside the District premises.

This policy applies to all District employees, contractors, consultants, temporary employees, and other staff at all District locations or who access District information resources remotely. It includes those staff affiliated with third parties who access District's computer networks. Throughout this document, the term staff will collectively refer to these individuals.

The policy also applies to all students who use or access the District's computer / telecommunications environment or any information, equipment or records that are owned by the District as part of class curriculum, for research as part of class work, as part of school extra curricular activity including but not limited to administrative assistance, clubs or committees, or as a privilege for personal use.

### **3. Functionality**

The District may make use of telecommunications and storage mechanisms that, if left unsecured, would put valuable information at risk.

The District uses or may use the public Internet for:

(List of uses that may include but are not limited to)

- Maintaining a web site that is currently used as an information-sharing device for the general public. Information sharing includes posting of schedules, event descriptions, posting of homework assignments, description of classroom activities and accomplishments.
- Email communication with parents, board members, PTA, vendors, other external business partners
- Distance Learning for staff and students
- Research by staff and students
- Communication with vendors and downloading of services and technology
- Partnering with vendors to enhance the use of technology in the District to reduce costs, improve service and provide expanded training and opportunity for students

The District also maintains Local Area Networks in each facility and a Wide Area Network which, in addition to providing Internet Access, is used for file sharing, operating and accessing both education and business applications and managing public, business only and confidential information. The District will store information both at District facilities and off-site.

### **4. Data**

Information in all its forms and through its life cycle will be protected from unauthorized modification, destruction, disclosure, or denial, whether accidental or intentional.

The types of information stored, processed, and exchanged by District include:

Student Directory Information  
Student Personally Identifiable Information  
Student Education Record Information  
Staff Confidential Information  
General District Information (ex: Schedules, Policies, Public Records)  
District Financial Information (ex: Banking, Budget, Investment, Payroll)  
District Property Information (ex: Security, Property records)  
District Operations Information (ex: Emergency evacuation, Food services, Transportation)

These types of information will be assigned to the following categories:

Public: Information that is freely releasable to the general public

- General District Information

Business Only: data that is generally releasable to staff as needed for use in their day-to-day operations as well as board, committees and others as appropriate.

- Student Directory Information
- District Operations Information

Confidential: data that may include sensitive, private, and/or proprietary information. This data must be protected from disclosure to, or modification by, unauthorized persons. It may only be disclosed to authorized persons (or roles) who have been specifically given permission to receive this information. Permission will be granted to staff that require access to the information in order to perform District job duties or complete District projects.

- Student Personally Identifiable Information
- Student Education Record Information
- Staff Confidential Information
- District Financial Information
- District Property Information

## 5. Roles

Every staff member and student is responsible for safeguarding District information and physical assets. Every staff member and student is also responsible for using resources in an effective, ethical, and lawful manner.

The following are general categories of users of District computer / telecommunication resources.

Students

Administrative Staff

    Commissioned Officer

    Management Staff

Professional Staff

    Management Staff

    Teaching Staff

    Education Assistants

Classified Staff

Regardless of role, a person has a particular relationship to a piece of information. They could be an Owner, a Custodian, or a User of that information (and possibly more than one).

## **5.1 Owners**

All information must have a designated owner. The owner will designate whether the information is confidential, business only, or public, and define which users are permitted access to the information, and define the authorized uses.

## **5.2 Custodians**

Custodians are in physical or logical possession of District information or information that has been entrusted to District. Custodians are responsible for ensuring the security of the information to prevent inappropriate disclosure. Custodians are also responsible for the backup of critical information so that it will not be lost. Custodians also must implement, operate, and maintain security measures defined by the information owner. The Technology Director and Technology Assistants are primary custodians. However, other administrative staff may be custodians of some business records; Teachers may be temporary custodians of student records, etc.

## **5.3 Users**

Users must acknowledge and comply with all District's policies, procedures, and standards dealing with information security. User's questions regarding the handling of specific information must be directed to the information owner.

## **6. Account Policy**

The term "account" refers to the granting of the privilege to access an operating system, network, or application. Creating an account is usually associated with the assignment of a user id. All accounts must be granted to individual persons (and not to roles or generic users).

User accounts for staff's access to District resources must be limited to people who are acting in roles that require access to those resources. Accounts will only be granted for specific machines and applications required. New accounts are granted per the New Account Procedure and must be approved by a Commissioned Officer or Management Staff. Accounts must be removed immediately when staff terminates employment or change roles. District staff must read the Telecommunications Acceptable Use Policy and sign the Staff Security Agreement before being granted access.

Student Accounts will have limited access. Accounts will be disabled when school is not in session. Students must read the Telecommunications Acceptable Use Policy and sign the Student Security Agreement before being granted access.

Users who have multiple roles may have multiple accounts. Users must use the appropriate account for the action they are executing (for instance, use of the root account must be extremely limited)

## **7. Access Policy**

Users have limited rights to access District information. They are only granted permission to access resources that they are required to use in performing their assigned role. All other access is denied by default. This is known as the “principal of least privilege”.

Information owners grant access rights. Information custodians control access. Access permissions for systems and directories must be set to prevent disclosure to unauthorized users.

Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file. The ability to read, modify, delete, or copy a file belonging to another user does not necessarily imply permission to actually perform these activities.

Users must be authenticated before being provided access to District operating systems, applications, and network operating systems.

Users who fill multiple roles may have multiple accounts. Users must authenticate using the appropriate account for the action they are executing (for instance, use of the root account must be extremely limited).

Where user ID and passwords are used to authenticate users, password usage will be subject to the Password Management Policy. Users must select a secure password and must not divulge that password to anyone.

Where encryption or other privacy technologies are used to protect information, use of those technologies and the Key Management Infrastructure to support them are subject to an Encryption (or other technology) Usage Policy. (Anticipated as a future requirement.)

District staff will be granted remote access privileges to specific District data residing on District’s internal network on an as required basis. (Anticipated as a future requirement) All remote access must be in compliance with the Remote Access Policy. Remote access to District resources must be employed such that the confidentiality and integrity of protected data is maintained.

## **8. Information Protection Policy**

Users handling District information must ensure the information is not disclosed to anyone who does not have the appropriate permission. This is true for the entire lifecycle of information:

- Storage
- Reproduction
- Transport
- Destruction

Information defined as confidential information must be protected throughout this lifecycle. Any transfer of confidential information must to an authenticated peer. Reproduction of confidential information is not permitted unless authorized by its owner. Likewise, extracts, summaries, or derivatives of confidential information cannot be made without approval of the owner.

## **9. Network Maintenance Policy**

The stability of the District network is critical to fulfilling its mission. All modifications to hardware and software must be approved according to the Network Maintenance Procedure. This procedure addresses:

- Configuration control
- Adding hardware
- Adding software to existing HW (new and upgrade)
- Changing configurations

All maintenance information and actions are considered confidential and must comply with the requirements for protecting confidential information.

Commercial software must be used in accordance with licensing agreements and copyright law. Personal software must not be installed on District servers. Installation of personal software on individual users' computers must be individually authorized and must follow the Personal Software Procedure.

Platforms and applications must be periodically subject to a security assessment and review of configuration. Platforms, and applications must be kept up to date with regards to security related patches and upgrades.

## **10. Privacy Policy**

Although it is not the intention of District to discover or disclose personal information within District's offices and premises, District reserves the right to access all information contained in electronic format on or distributed by means of the computer and/or telephone equipment at District, whether directly or indirectly related to the business of District or otherwise personal to the employee. District staff are required to comply with all federal, state and local, regulations and laws regarding student privacy as well as District policies regarding privacy, harassment and acceptable use.

### **10.1 Remote Assistance**

Information Technology Director, Assistant Information Technology Director and support personnel selected by the Superintendent of the district or his/her designee have the right to offer remote assistance to the users requesting hardware and or software support for their desktops. Remote assistance will include desktop control and manipulation of settings and data residing on the computer relevant to the issue at hand. Access rights during remote assistance are limited to the issue only and all staff members must authorize remote assistance before it is initiated. In case of student level users, authorization is not necessary.

## **11. Physical Access**

Physical access to the District telecommunications network is managed through the Building Security Policy. Access to building areas where computer / telecommunications equipment reside will be strictly managed.

## **12. Incident Handling**

Any incident regarding the security integrity of District computer / telecommunications equipment or data resources must be reported to IT Management immediately. This includes any failure to follow District policy as well as attempted attacks on or intrusions into District resources. IT Management will invoke the Incident Handling Procedure, to react to, escalate, and investigate the incident. IT Management will schedule periodic drills to assure appropriate reaction to security incidents.

**13. Disaster Recovery**

Management must maintain a Disaster Contingency Plan. All operations information must be backed up and stored off-site. The backup procedure is captured in the Data Backup Process. IT Management will schedule maintenance and periodic drills to assure the ability to maintain business operations in the event of a disaster.

**14. Security Awareness**

The superintendent's office must ensure that all District staff and students are aware of, have access to, and comply with the District Security Policy. It must ensure that all District staff receives security-awareness training upon employment and periodically thereafter.

**15. Compliance**

The violator of the District's security measures will be responsible for damages to equipment, systems and software resulting from deliberate or willful acts. General rules of behavior and communications apply when using the telecommunications / computing environment including all policies related to privacy, harassment, vandalism and theft.

In the event that a staff member or student violates any of the District's security measures, the Incident Handling Policy covers investigation of any such incident. A substantiated charge of non-compliance against a staff member or student shall subject such staff member or student to restriction of use or access to computer / telecommunications resources and/or other disciplinary action up to and including discharge or expulsion. Illegal use of the telecommunications / computing environment, deletion or damaging of files or data, copyright violations, theft of services, hacking, or bypassing security controls, violations of the privacy standards of another user, student, staff or the district or misrepresentation of another's identity, or vandalism, will be reported to the appropriate legal authorities for possible prosecution

Adopted: April 22, 2003

Revisions adopted: May 23, 2006 effective July 1, 2006