Overview

Information technology (IT) security and integrity are critical to the instruction and operations of the district. The following list provides insight into some of the reasons for IT security and to show the depth and breadth of information resources that need protection. This list is representative and is not meant to suggest the full range of information and resources that must be protected.

Support and maintain the ongoing functions: As an increasing percentage of the district's functions are handled electronically, it is critical that information and information systems be protected so the district can operate without interruption.

Protect district assets: The district is in possession of many assets including, but not limited to, instructional and student data, copywrited software and physical assets. Loss of these assets could have significant financial impact as well as a major negative impact on instructional programs and administrative functions.

Safeguard the privacy of individuals and information: With the increasing risk of identity fraud and other potential misuses of personal information, it is paramount the district safeguard personal information entrusted to the district.

Protect the integrity and reputation of the district: Security breaches, misuse of district assets and non-educational uses of district resources reflect negatively on the capability of the district to manage the resources entrusted to it. In addition, security breaches could result in the potential for criminal or civil action.

Comply with state and federal laws: State and federal laws and regulations require the district to take reasonable steps to ensure the security of the data (e.g., FERPA, HIPAA, CIPA). Failure to safeguard this information and filter inapropriate Internet information could result in legal action or cause the district to lose its ability to offer certain services.

Objectives

The four primary objectives of Information Technology security are to protect:

Confidentiality of information: Preserving the privacy of personal and other district information for authorized uses only; preserving the rights of ownership associated with intellectual property (e.g., copyright, trademark, license).

Integrity of data: Assuring the reliability of data by preventing unauthorized or inadvertent modification or deletion of data.

Availability of resources: Ensuring timely and reliable access to and use of data and information technology resources.

Authorized use of resources: Preserving the use of information resources for authorized use and preventing the malicious or inapropriate use of information resources.

Definition of Terms

Damage or impairment to district IT resources: The use of or allowing the use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently (1) damaging any system, (2) damaging or violating the privacy of information not belonging to you, or (3) misusing or allowing the misuse of any district resources.

Use of or allowing the use of any district resources for non-district related activities that unduly increase network load (e.g., chain mail, on-line shopping, investments, radio, fantasy sports leagues, playing/downloading music, and non-approved or non-educational games)

Use of or allowing the use of any system resources in a manner inconsistent with the district's educational goals and objectives.

Unauthorized commercial activities: Using district resources for one's own commercial gain, or for other commercial purposes not officially approved by the district.

Using district resources to operate or support a non-district related business.

Enforcement

Overview

The Director of Technology is responsible for protecting the system and users from abuses of this policy. Pursuant to this duty, the Director of Technology may informally or formally communicate with offending users. In more extreme cases, the Director of Technology may temporarily revoke or modify use privileges. Temporary suspension decisions are reviewable by the building administrator and ultimately the Superintendent.

Abuse, misuse or allowing the misuse of district resources violates this policy, but it may also violate the criminal statutes. Therefore, the district will take appropriate action in response to user abuse or misuse of computing services. Action may include, but not necessarily be limited to:

- suspension or revocation of computing resources, access to all computing facilities and systems can, may, or will be denied;
- reimbursement to the district for resources consumed;
- other legal action including action to recover damages;
- referral to law enforcement authorities;
- computer users (faculty, staff and/or students) will be referred to the appropriate administrator(s)/board for disciplinary action.

Minor Infractions

Minor infractions of this policy, when likely accidental in nature, such as poorly chosen passwords, overloading/impairing systems (e.g., on-line games or recreational use) and other minor offenses, are typically handled in an informal manner by electronic mail or in-person discussions. More serious infractions or repeated minor infractions are handled via formal procedures.

Minor infractions include, but are not limited to:

- using another person's account or attempting to capture/guess other users' passwords;
- searching for inappropriate Internet content (violation of the Federal Childrens' Internet Protection Act - CIPA);
- trying to obscure your true identity as the sender of electronic mail, message posting or the user of other networked services that require identification/login;
- using district computing resources for unauthorized commercial purposes;
- violating terms of applicable software licensing agreements or copyright laws.

Repeated Minor Infractions and Serious Misconduct

Infractions such as harassment, circumventing normal log-on procedures and security regulations or repeated minor infractions as described in, but not limited to, the above policies will result in the temporary or permanent loss or modification of computer access, and notification of the appropriate administrator(s), parents/guardians and/or law enforcement authorities. Repeated minor and more serious infractions will result in Memorandums for Record, and may warrant disciplinary and/or legal action.

Warning! Loss of the use of district computers and resources, even if temporary, may prevent a student from completing course assignments and from making normal progress in the course. This is very likely to have a negative impact on the final course grade, and the acceptance of make up work is left to the discretion of the course teacher.

Violation of Local, State or Federal Laws

Offenses which are in violation of local, state or federal laws will result in the immediate loss of all computing access, and will be reported to the appropriate district, parent/guardian and law enforcement authorities.

Questions Relating to This Policy

The examples of unauthorized use set forth in this document are not meant to be exhaustive. Additional questions about this policy or of the applicability of this policy to a particular situation should be referred to your building Principal who will involve the Director of Technology and/or Superintendent if necessary. The Superintendent is the final authority on questions of appropriate use of district resources. Whenever you are in doubt regarding an issue of questionable use, it is in your best interest to resolve the issue before pursuing any questionable use of district resources.