TECHNOLOGY SECURITY POLICY

The District will strive to provide equal opportunities for the use of technology. The District is responsible for supporting initiatives that balance security, privacy, educates data custodians in laws and regulations and provides a productive teaching/learning environment. The District is also responsible for purchasing hardware and software that meets or exceeds current District standards.

The IT Department is responsible for:

A. Establishing and maintaining up to date organization-wide information security policies, standards, guidelines, and procedures.

B. Investigations of system intrusions and other information security incidents.

C. Providing an updated list of supported standards for computing resources at least annually. This includes maintaining a list of approved and supported software and hardware. If the software/hardware is not on the approved software/hardware list, IT will test to determine if it can be supported based on current specification and potential conflicts with other software.

D. Purchasing and maintaining hardware that meets or exceeds current District hardware standards.

E. Patching and updating systems in a test environment first and then deploying the updates in production.

F. Obtaining the latest anti-virus signatures and software updates.

G. Participating in any major application deployments or infrastructure changes to ensure security features are incorporated.

H. Developing and presenting security awareness programs to students and faculty.

I. Account Management.

J. Monitoring of system access.

District Employees are responsible for:

A. Supervising their scheduled lab environments to ensure that systems are not abused. For example, teachers must monitor the systems to prevent removal or damage of software or hardware components such as a system mouse.

B. Ensuring that any software they install on a District system is licensed.

C. Reporting any malicious activity.

D. Ensuring the confidentiality of student data to which teachers have access.

Refer to the Family Educational Rights and Privacy Act (FERPA) Student Records Policy 6.16 for additional Teacher Responsibilities.

Students are responsible for:

A. Acknowledging and adhering to District Policy (including the Acceptable Use of Computing Resources).

B. Reporting any security events including viruses.

Refer to the Family Educational Rights and Privacy Act (FERPA) Student Records Policy 6.16 for additional Student Responsibilities.

Parents or Guardians are responsible for:

A. Acknowledging school policy and the Acceptable Use of District computing resources for any student under age 18.

B. Co-signing the agreement that defines responsible and ethical use of computing systems and agreement, if student is not yet 18 years old.

Refer to the Family Educational Rights and Privacy Act (FERPA) Student Records Policy 6.16 for additional Parent/Guardian Responsibilities.

All users are responsible for adhering to District Policy. Questions regarding the handling of specific types of information can be directed to the IT Department or the owner of the information.

Users are responsible for:

A. Ensuring software loaded on their systems is licensed.

B. Reporting malicious activity.

C. Maintaining confidentiality of student and staff data in compliance with District Policy and any state and federal regulations.

IT shall use the latest technological means to include, at a minimum, virus scanning software obtained from an industry proven leader in order to prevent information systems infection by malicious code. Users will be made aware of the dangers that malicious code presents to software and data. All District computers will have current versions of antivirus software with scans being executed at least daily. Virus scanning will be performed against all incoming and outgoing email.

Users shall not knowingly create, execute, forward, or introduce any code designed to self replicate, hide itself, damage or degrade the overall performance of MPS's information system. Additionally, users shall not use MPS's systems to transmit the code over the network to infect any other organization's information systems.

The Network and all information, content, and files are the property of the District. Users should not have any expectation of privacy regarding those materials.

All access to the District's computing resources and network will require an account consisting of a unique username and password. The username identifies the user, authorizing the applicable level of computer resources and network access. The password authenticates the username. All accounts created will have a request and approval process, with the appropriate access level assigned to the computer resources. Users will be required to sign the MPS Acceptable Use form.

Users shall be held accountable for the use or misuse of computer resources. Every user is responsible for activities performed by their personal account and must protect their password to prevent undesirable activity.

IT will assign an initial default password to be used for initial logon only. This password must be changed at initial logon. The new password must adhere to the "Password Requirements" as stated below.

Passwords must not be written down and left in a place where an unauthorized person might discover them. They must also not be stored near the device for which they pertain. Sharing of passwords is strictly prohibited. If users need to share information, several methods are available such as electronic mail, databases, diskettes, and public files stored on local area network servers.

System logging (auditing) will be enabled for all systems that provide such a feature to record, at a minimum, failed login access to a server. Information that must be logged should include date, time, username and a description of the event. System logs will be retained for a minimum of 1 month. These logs can be kept online or archived on other storage media. Access to system and network logs will be controlled by IT.

Students, staff, and vendors are not allowed to connect the following devisees to MPS's network:

A. Unauthorized modems,

B. Wireless networking equipment,

C. Personal Digital Assistants,

D. Virtual Private Networks (VPN),

E. Remote control software,

F. ISP (Internet Service Provider) Software,

G. And any other software or hardware that connects to unapproved external networks.

Approval from the IT must be obtained before systems defined as "Not Owned and Not Maintained by MPS" are connected to the Mentor network.

Appropriate approvals and a signed "Network Acceptable Use Agreement Form" are required by any user who accesses a system remotely.

Wireless Access Points must be approved by and meet the IT security requirements and receiver standards. The IT Department has the right to monitor the network for any rogue Wireless Access Points and terminate the connection.

Updates and patches will be applied to strategic system software in an appropriate amount of time once a need has been identified and thoroughly tested. The IT is responsible for a reliable notification method for current update and patch releases and applying them when needed.

Access to the computer room and wiring closets will be physically restricted by a controlled method. Staff members with privileges to secure locations are responsible for the security of their access devices (i.e., keys, access cards, etc.). Logs of access to secure locations will be maintained. The IT will maintain access rights to the data center(s) room, network wiring racks and any other facilities where critical computing equipment is housed.

Adopted: July 18, 2006