SUBJECT: DATA NETWORKS AND SECURITY ACCESS

The District values the protection of private information of individuals in accordance with applicable law, regulations, and best practice. Accordingly, District officials and Information Technology (IT) staff will plan, implement, and monitor IT security mechanisms, procedures, and technologies necessary to prevent improper or illegal disclosure, modification, or denial of sensitive information in the District Computer System (DCS). Similarly, IT mechanisms and procedures will also be implemented in order to safeguard District technology resources, including computer hardware and software. District network administrators may review District computers to maintain system integrity and to ensure that individuals are using the system responsibly. Users should not expect that anything stored on school computers or networks will be private.

In order to achieve the objectives of this policy, the Board entrusts the Superintendent or Data Privacy Information Officer to:

a)   Inventory and classify personal, private, and sensitive information on the DCS to protect the confidentiality, integrity, and availability of information;

b)   Develop password standards for all users inc   O District's network operating
em, which will allow the District to determine on a constant basis who is accessing the
, and establish procedures for periodically reviewing audit trails;

elop procedures to control physical access to computer facilities, data rooms, systems,
vorks, and data to only authorized individuals; these procedures may include ensuring
server rooms remain locked at all times and the recording of arrival and departure dates
times of employees and visitors to and from the server room

riodically grant, change, and terminate user access rights to the overall networked
mputer system and to specific software applications and ensure that users are given access
sed on, and necessary for, their job duties;

mit user access to the vendor master file, which contains a list of vendors from which
strict employees are permitted to purchase goods and services, to only the individual who
responsible for making changes to this list, and ensure that all former employees' access
ghts to the vendor master list are promptly removed;

(Continued)

SUBJECT: DATA NETWORKS AND SECURITY ACCESS (Cont'd.)

h)   Determine how, and to whom, remote access should be granted, obtain written agreements with remote access users to establish the District's needs and expectations, as appropriate, and monitor and control remote access;

i)   Verify that laptop computer systems assigned to teachers and administrators use full-disk encryption software to protect against loss of sensitive data;

j)   Deploy software to servers and workstations to identify and eradicate malicious software attacks such as viruses and malware;

k)   Develop a disaster recovery plan appropriate for the size and complexity of District IT operations to ensure continuous critical IT services in the event of any sudden, catastrophic event, including, but not limited to fire, computer virus, or deliberate or inadvertent employee action.

Password Guidelines

Passwords are an important way to protect the security of the DCS and maintain the integrity of sensitive or confidential data. Therefore, in order to ensure the security of the DCS, users must comply with the following:

1. Choosing Passwords

The initial password provided to a system user must be changed by the user immediately upon gaining access to the system for the first time. Passwords must contain at least twelve (12) characters, a mixture of upper and lowercase letters, and at least one number. Such passwords should not be a common words, family or pet name, address, birthday, social security, or telephone number. When a passport is reset, it should not duplicate the previous passwords. In addition, user account will lock after three unsuccessful attempts to log on to the DCS.

2. Changing Passwords

Employees of the District must change their network passwords every 90 days. Each password is secured by the individual users and maintained by the Office of Technology.

All system level passwords will be changed whenever a member of the Information Technology (IT) staff changes. All user level passwords for network access will be changed when a compromise is suspected.

(Continued)

SUBJECT: DATA NETWORKS AND SECURITY ACCESS (Cont'd.)

3. <u>Password Sharing</u>

Passwords should not be shared under any circumstances. If access is required by a supervisor, the system administrator will change the user's password to permit access. When the user returns to work, the password can be reset by the user.