

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, such 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 his or her designee, 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;
- c) Ensure that the "audit trail" function is enabled within the District's network operating system, which will allow the District to determine on a constant basis who is accessing the DCS, and establish procedures for periodically reviewing such audit trails;
- d) Develop procedures to control physical access to computer facilities, data rooms, systems, networks, and data to only authorized individuals;
- e) Establish procedures for tagging new purchases as they occur, relocating assets, updating the inventory list, performing periodic physical inventories, and investigating any differences in an effort to prevent unauthorized and/or malicious access to these assets;
- f) Periodically audit user access rights to the overall networked computer system and to specific software applications and ensure that users are given access based on, and necessary for, their job duties;
- g) Verify that laptop computer systems assigned to teachers and administrators use full-disk encryption software to protect against loss of sensitive data;
- h) Deploy software to servers and workstations to identify and eradicate malicious software attacks such as viruses and malware;
- i) 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.

Adopted: 6/20/17