Code: EHAA

ACCEPTABLE USE POLICY

Purpose:
The purpose is to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access sensitive information.

Scope:
This policy applies to all District workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information. In addition, this policy applies to all workstations and other computing devices owned or operated by the District and any computing device allowed to connect to the District's internal network.

Policy:
The workstations and other computing devices at the District are to be used for work related purposes except as otherwise provided. This includes, but is not limited to, Internet and Web access as well as the use of e-mail at the District. Workforce members should not expect any level of privacy as their activities, e-mails, files, and logs may be viewed at any time by the Security Officer or other members of management in support of this and other policies and procedures.

The District may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems.

The District will implement reasonable and appropriate measures to secure its computing devices could be used to access sensitive information. These measures will include, but are not limited to the following:

- All user and administrator accounts must be protected by some form of authentication. If passwords are used, they must follow the guidelines set forth in the Authentication Policy.
- All users accessing the District computing devices must have and use a unique user ID as set forth in the Authentication Policy.
- Procedures must be maintained that implement security updates and software patches in a timely manner.
- Procedures must be maintained that require users to run an up-to-date anti-virus program on all computing devices at the District.
- All unnecessary and unused services (or ports) must be disabled
- Measures will be taken to physically protect computers that are located in public areas and portable computers such as laptops and PDAs that can be taken off the premises.
- Computers located in public areas will be situated as to block unauthorized viewing and/or will have screen savers that black out the screen.

Responsibilities:
The Technology Co-Coordinator will be responsible for ensuring the implementation of the requirements of this policy.

Compliance:
Failure to comply with this or any other security policy will result in disciplinary actions up to and including termination of employment. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Adoption Date: December 11, 2017