Appropriate Use of District Technology, Network Systems, and Internet Access

The District requires employees and students to learn to use computing devices, data networks, enterprise software systems, electronic mail, the Internet, and telecommunications tools and apply them in the appropriate ways to the performance of tasks associated with their positions and assignments.

Students and employees shall only engage in appropriate, ethical, and legal utilization of the District's technology, network systems, and internet access. Student instruction on digital citizenship standards which includes safe, ethical, and responsible use of the Internet will be defined and taught within core curriculum. Student and employee use of the District's technology, network systems, and internet access shall also comply with all District policies and regulations.

The following rules provide guidance to students and employees for the appropriate use of the District's technology, network systems, and internet access. Inappropriate use and/or access will result in the restriction and/or termination of the privilege of access to and use of the District's technology, network systems, and internet access and may result in further discipline for students up to and including expulsion and/or other legal action and may result in further discipline for employees up to and including termination of employment and/or other legal action. The District's administration will determine what constitutes inappropriate use and their decision will be final.

Inappropriate use includes, but is not limited to:

- Uses which violate any local, state or federal statute or regulation.
- Creating, accessing, uploading, downloading, transmitting or distributing pornographic, obscene, profane, abusive, threatening, sexually explicit or otherwise inappropriate material, or material encouraging or promoting discrimination towards individuals or groups of individuals based upon a legally protected trait or characteristic.
- Uses which violate copyright laws or otherwise misuse of the intellectual property of another individual or organization.
- Accessing another individual's materials, information, or files without authorization (authority).
- Any unauthorized access or malicious attempts to damage hardware/software or networks, circumvent or disable security protocols, or to destroy the data of another user, including creating, loading or intentionally introducing viruses.
- Altering the operation of computing devices as set by the network administrator.
- Using computing devices, data network or Internet for commercial purposes, or personal purposes which interfere with job performance or function of the workplace, or other purposes not consistent with the educational objectives of the District.
- Using the system to communicate, publish or display defamatory materials, rumors, disparaging portrayals or any other information which is known to be false or misleading.
- Harassing, insulting, or threatening harm or embarrassment of others.
- Swearing or using vulgarities or any other inappropriate language.
- Disseminating or soliciting sexually oriented messages or images.
- Disabling, circumventing or attempting to disable or circumvent filtering software.
- Transmitting personal credit card information or other personal identification information.
- Invading the privacy of individuals without authorization.
- Failing to follow District policy while using computing devices, data networks or accessing the Internet; or failing to follow any other policies or guidelines established by District administration or the employee's supervisor and failure to follow instructions of supervisors.

Individuals should not allow anyone else to use their assigned login credentials or passwords to access or use the District's computing devices, data network, information systems or the Internet. Users are responsible for the security of their own e-mail, computer and data network access. Users will be held responsible for any misuse of their computing device, e-mail or data network access by themselves or by others when the user has failed to follow appropriate security measures.

Employees authorized to allow student access to the District's data network and Internet may do so only according to this policy and are responsible for supervising student access. Employees who allow student access to computer networks and the Internet in violation of this policy may be subject to disciplinary action up to and including termination.

Employees are responsible for maintaining a safe and secure school environment. This includes computing devices and the data network. All users will routinely change passwords when required or directed by system administrators. Staff will assist students with password changes as needed. Users determined to be a security risk may have access restrictions applied.

Approved: 06-11-18