ACCEPTABLE USE OF DISTRICT TECHNOLOGY RESOURCES BY PROFESSIONAL AND BUSINESS USERS

1. Definitions and Introduction

This policy establishes the framework for acceptable use of district technology resources and applies to all users.

The term "district technology resources" includes, but is not limited to, computer and telephony hardware and systems, software applications, internal networks and Internet access, stored data, and related services such as email and voice mail, including any that are provided by a third party, such as BOCES.

The term "users" includes, but is not limited to, full-time, part-time, and temporary employees, independent consultants, contractors, vendors, and volunteers (hereinafter collectively referred to as "all users" or "users").

District technology resources, and all communications and stored information transmitted, received or contained therein, are district property and are to be used for job-related purposes and educational purposes. The district may access and monitor these resources to ensure that such equipment is used for proper purposes. There is no assumption of privacy. All users are on notice that communications are not private. The existence of a staff member pass code or password does not mean that messages or data are confidential.

Users are prohibited from using pass codes, accessing files, or retrieving any stored communication without prior authorization.

All users are responsible for the content of all text, audio and visual images that they create or transmit using district technology resources. No email or other electronic communications may be sent which hides the identity of the sender, or represents the sender as someone else or someone from another organization. Messages must include the sender's name.

2. Acceptable Uses

District technology resources are intended for business and educational use and to facilitate communication with the public, and thus are expected to be used in a productive, professional manner.

3. Unacceptable Uses

A. Personal Uses

District technology resources shall not be used for outside business ventures, personal gain, organizational campaigns, or political or religious causes, and any such use is prohibited.

B. Offensive Content

District technology resources may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated, or for any purpose against the district's policies or best interest. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, gender, or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted. All users are prohibited from downloading, viewing, transmitting and/or possessing obscene, pornographic, profane, sexually explicit, or racially offensive materials with such terms having the meaning given to them by statute, case law or by common usage and understanding in the community.

C. Unauthorized Downloading or Installation of Software

Unauthorized downloading or installation of any software, whether from the Internet or any other source, is prohibited.

D. Privacy and Unauthorized Access

Users are prohibited from accessing or attempting to access any stored information or communications without appropriate authorization.

E. Violations of Law

Illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity must be reported to the proper authorities. Transmission or use of any material in violation of any federal, state or local law or regulation is prohibited. This includes, but is not limited to, materials protected by privacy, copyright, trade secret, property right, and intellectual property right laws.

4. Monitoring

All users are hereby put on notice that any and all use of district technology resources may be monitored, and all messages and files created, sent, stored or retrieved are property of the district and are subject to inspection without notice. All users are put on notice that system security features, such as passwords and message delete functions, do not take away the ability to archive any message or file, at any time, for future viewing.

5. Reporting Security Problems

Users must notify the district when any district technology resources or district data is lost or disclosed to unauthorized parties, unauthorized use has taken place, passwords or other system access control mechanisms are lost, stolen, or disclosed, or any of the preceding is suspected to have happened. Unusual system behavior should also be reported.

6. Expenses

Users are prohibited from using district technology resources in any manner which results in unauthorized charges or expense to the district.

7. Expiration of Email

Email stored on district email servers may be deleted, on a periodic basis, at the convenience of the district and in compliance with the records retention laws applicable to public entities.

8. Sanctions

Failure to comply with district policy or regulation may result in suspension and/or revocation of access privileges as well as discipline up to and including discharge.

9. Disclaimer

The district makes no warranties of any kind, neither expressed nor implied, regarding district technology resources and shall not be responsible for any damages users suffer, including, but not limited to, loss of data resulting from delays or interruptions in service. The district shall not be responsible for the accuracy, nature, or quality of information gathered or stored through use of district technology resources. The district shall not be responsible for personal property used to access district technology resources. The district shall not be responsible for unauthorized financial obligations resulting from district provided access to the Internet.

10. Law

This policy and all its provisions are subordinate to local, state, and federal laws.

Adopted: July 15, 2013