POLICY	**9575** **Adopted: May 6, 2014** **Personnel & Negotiations**

SUBJECT: E-MAIL ACCEPTABLE USE POLICY

Purposes and Goals

E-mail is one of the BOCES' core internal and external communication methods. The purpose of this policy is to ensure that e-mail systems used by BOCES staff support BOCES business functions to their fullest capacity. This policy notifies staff of their responsibilities and provides direction in managing information communicated by e-mail. For purposes of this policy, the terms "staff" and "user" shall be deemed to refer to all BOCES employees and officials who are granted access to e-mail services, including, but not limited to, full-time employees, long-term substitutes, and elected officials.

Access to E-mail Services

E-mail services are provided to all BOCES staff whose job functions and responsibilities require such services, as determined by their supervisor and the Administrator of Technology Solutions. Long-term substitutes are permitted to have e-mail access only while serving in such capacity.

Use of E-mail

E-mail services, like other means of communication, are to be used to support BOCES business.

- Staff **will not use** e-mail for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of the BOCES.
- E-mail sent to recipients outside the BOCES is unencrypted and unsecure and should not contain confidential information (such as protected information as defined by HIPAA or FERPA). Specifically, no staff member may send an e-mail message with any individual's social security number.
- Users with a BOCES e-mail account may use only this account and not a personal e-mail account to conduct official business of the BOCES. Administrators and Board of Education members are required to use BOCES e-mail in the conduct of official public business.

Privacy and Access

E-mail messages are neither personal nor private. E-mail system administrators will take reasonable precautions to protect the privacy of e-mail. However, supervisors and technical staff may access an employee’s e-mail:

- for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time);
- to diagnose and resolve technical problems involving system hardware, software or communications; and/or
- to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists, or in conjunction with an approved investigation.

E-mail messages sent or received in conjunction with District business may be subject to release under the Freedom of Information Law.

All e-mail messages, *including personal communications*, may be subject to discovery proceedings in legal actions.

Security

E-mail security is a joint responsibility of BOCES technical staff and e-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their accounts by unauthorized individuals.

All e-mail users must be familiar with the following terms:

- ***Phishing*** is a common technique used to trick a person into providing personal information such as his or her username, password, social security number and financial information. This information should ALWAYS be kept secure and confidential, never included in an e-mail message, and never provided to a website that requests it after clicking on a link in an e-mail message. If a user has any doubt as to the authenticity of a request for this information, contact the helpdesk for verification.

- ***Malware*** is a category of malicious software that includes adware, spyware, viruses, worms and Trojans. Malware frequently is distributed by e-mail by convincing a user to click a link or open an attachment in an e-mail message that will transmit malware to the machine, infecting the machine. Infected machines can spread the infection to other computers and networks. Users must not click a link or open an attachment in an e-mail message unless they can verify that it is safe by verifying the sender of the message (see "Spoofing" below) and understand the sender's reason and intent for sending the message. Users must never click a link in an e-mail message that is only a link with no other content. If a user suspects that a machine has become infected with malware, he or she must turn the machine off to prevent the spread of the infection and report it to the helpdesk.
- ***Spoofing*** is a common technique employed by malware and hackers that involves misrepresenting the sender of a message by changing the sending name and address. Users may receive messages from people that they know and trust that may not actually originate from those people. These types of spoofed messages are usually an attempt to obtain information by phishing or infecting the machine with malware by convincing the user to click a link or open an attachment. Messages that are received that have spoofed sender information must be deleted. If a user is unsure if the message is legitimate, he or she should contact the helpdesk.

Management and Retention of E-mail Communications

All incoming, outgoing and inter-BOCES e-mail is archived using a mail archiver server managed by Computer Services. The mail archiver will retain all e-mail records for a period of six (6) years to comply with records retention and disposition requirements under Schedule ED-1. The mail archiver will automatically delete and permanently destroy e-mail records six (6) years after they are created unless a legal hold has been placed on the records.

Any e-mail records that need to be retained for a period that is longer than six (6) years (permanent records) need to be transferred by the e-mail user from the mail system or the mail archiver to a paper filing system.

POLICY	**9575** **Adopted: May 6, 2014** **Personnel & Negotiations**

Records Retention

E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements and need to be retained by the BOCES for six (6) years.

Examples of messages and information sent by e-mail that typically are subject to this requirement include:

- policies and directives;
- correspondence or memoranda related to official business;
- work schedules and assignments;
- agendas and minutes of meetings;
- drafts of documents that are circulated for comment or approval;
- any document that initiates, authorizes, or completes a business transaction;
- final reports or recommendations.

Some examples of messages that typically do not constitute records are:

- personal messages and announcements;
- copies or extracts of documents distributed for convenience or reference;
- phone message slips;
- announcements of social events.

Due to the implementation of the mail archiver server, e-mail users do not need to be concerned with retention of records that only need to be retained for six (6) years, but are advised that messages that are not records also are retained for six (6) years.

Users are responsible for the retention of any e-mail message that qualifies as a "permanent record" according to Schedule ED-1 in the event the e-mail message is the only copy of the permanent record.

Computer Services will not retain backup tapes or backup media of the e-mail system for a period longer than six (6) years.