Personnel

SUBJECT: Email Acceptable Use and Responsibilities

Purposes and Goals

Email is one of the Elmira City School District's core internal and external communication methods. The purpose of this policy is to ensure that email systems used by District staff and management support District business functions to their fullest capacity. This policy advises staff and management of their responsibilities and provides guidance in managing information communicated by email. For purposes of this policy, the terms "staff" and "user" shall be deemed to refer to all District employees and officials who are granted access to email services, including, but not limited to, full-time faculty and staff, long-term substitutes, administrators and elected officials.

Access to Email Services

Email services are provided to all Elmira City School District staff whose job functions and responsibilities require such services, as determined by their supervisor, the Director of Administration and the Technology Director. Long-term substitutes are permitted to have email access only while serving in such capacity. To request access, staff must contact Human Resources to complete the Network User Authorization Form and sign to accept the District's Acceptable Use Policy. The Network User Authorization Form then will be forwarded to the Technology Director for approval.

Use of Email

Email services, like other means of communication, are to be used to support District business.

- Staff may use email to communicate informally with others in the District so long as the communication meets professional standards of conduct.
- Staff may use email to communicate outside of the District when such communications are related to legitimate business activities and are within their job assignments or responsibilities.
- Staff **will not use** email for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of the Elmira City School District.
- Email sent to recipients outside the District is unencrypted and unsecure and should not contain confidential information (such as protected information as defined by HIPAA or FERPA). Specifically, do not include in an email message any individual's social security number.
- Users with a District email account should use only this account and not a personal email account to conduct official business of the District. Administrators and board of education members are required to use District email in the conduct of official public business.

Privacy and Access

SUBJECT: Email Acceptable Use and Responsibilities

Email messages are not personal and private. Email system administrators will not routinely monitor staff members' email and will take reasonable precautions to protect the privacy of email. However, supervisors and technical staff may access an employee's email:

- 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 email when a reasonable suspicion of abuse exists, or in conjunction with an approved investigation.

A staff member is prohibited from accessing another user's email without the user's permission.

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

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

Security

Email security is a joint responsibility of District technical staff and email users. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their accounts by unauthorized individuals.

All email users should 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 email message, and never provided to a website that requests it after clicking on a link in an email 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 email by convincing a user to click a link or open an attachment in an email message that will transmit malware to the machine, infecting the machine. Infected machines can spread the infection to other computers and networks. Users are advised not to click a link or open an attachment in an email 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 should never click a link in an email 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 should 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 are advised that they 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 should be deleted. If a user is unsure if the message is legitimate, he or she should contact the helpdesk.

Management and Retention of Email Communications

Since email is a communications system, messages should not be retained for extended periods of time. Users should remove all email communications in a timely fashion. If a user needs to retain information in an email message for an extended period, he or she should transfer it from the email system to an appropriate electronic or other filing system. Email administrators are authorized to remove any information retained in the email system that is more than 365 days old and shall remove any emails that are more than five (5) years old.

All incoming, outgoing and inter-District email is archived using a mail archiver server managed by Technology Services. The mail archiver will retain all email 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 email records six (6) years after they are created unless a legal hold has been placed on the records.

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

Records Retention

Email 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 District for six (6) years.

SUBJECT: Email Acceptable Use and Responsibilities

Examples of messages and information sent by email 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, email 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 email message that qualifies as a "permanent record" according to Schedule ED-1 in the event the email message is the only copy of the permanent record.

Technology Services will not retain backup tapes or backup media of the email system for a period longer than six (6) years.

Roles and Responsibilities

District administration will ensure that policies are implemented by principals and supervisors.

Principals and supervisors will develop and/or publicize record keeping practices in their area of responsibility that address the routing, formatting and filing of records communicated via email. They will train staff in appropriate use and be responsible for ensuring proper usage and the security of physical devices and passwords.

SUBJECT: Email Acceptable Use and Responsibilities

District network administrators and internal control (and/or internal audit) staff are responsible for email security, backup and disaster recovery.

All email users should:

- Be courteous and follow accepted standards of etiquette;
- Recognize the use of District email;
- Protect others' privacy and confidentiality;
- Consider organizational access before sending, filing or destroying email messages;
- Protect their passwords;
- Remove personal messages, transient records and reference copies in a timely manner;
- Comply with District policies, procedures and standards.

Policy Review and Update

The Records Advisory Committee or designee will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be directed to the Technology Director or the Records Management Officer.

Adopted: 11/7/12