

**Section J - Use of the Glenbrook Electronic Messaging System**

The Board of Education acknowledges the need for electronic messaging as an efficient communication tool. This section explains the district's policies and procedures for the Glenbrook Electronic Messaging System (hereafter referred to as "e-mail"). Users need to understand privacy and security issues that apply to e-mail, as well as understand their responsibilities to use the e-mail system efficiently so that minimal service disruptions occur.

This document applies only to e-mail in its electronic form, including e-mail headers, transaction summaries, addresses, and addressees. It does not apply to printed copies of e-mail.

**1. Uses and Ownership**

Any e-mail address or account established on the Glenbrook High School District 225 Network is the property of Glenbrook High School District 225. E-mail users shall not expressly or implicitly give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the district unless appropriately authorized to do so. Users shall not employ a false identity.

**2. Usage Guidelines**

E-mail users shall not send or forward e-mail chain letters, "spam" (the widespread distribution of unsolicited e-mail), or "letter-bombs" (sending the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail), and shall not knowingly forward a "virus" or any other form of distribution which obstructs, diverts or otherwise interferes with the e-mail system.

Notwithstanding anything in this policy to the contrary, the district e-mail service may be used for incidental personal purposes. E-mail records arising from personal use are still deemed to be property of Glenbrook High School District 225.

Personal use must not:

- a. Directly or indirectly interfere with the operation of district computing facilities or electronic mail services;
- b. Burden the district with noticeable incremental cost;
- c. Interfere with the e-mail user's employment or other obligations to the district; or
- d. Contain inappropriate content or otherwise violate this policy.

The district e-mail service may not be used for:

- a. Unlawful activities or the promotion of unlawful activities;
- b. Commercial purposes not under the auspices of the district; or
- c. Uses that violate other Glenbrook High School District 225 Board Policies or Procedures.

**3. Confidentiality**

The security and confidentiality of electronic mail cannot be guaranteed and all e-mail remains the property of the District. Furthermore, administrators of e-mail services shall be deemed to have no control over the security of e-mail that has been downloaded to a user's computer.

Users of the district e-mail system should be aware that the *Freedom of Information Act* and other similar laws may require disclosure of e-mail, and may jeopardize the ability of the district to guarantee complete protection of any e-mail resident on district facilities. Users, therefore, should exercise extreme caution in using e-mail to communicate confidential or sensitive matters.

#### 4. Exceptions

During the performance of their duties, district system administrators have the authority from time to time to observe message header information to ensure proper functioning of the e-mail service, and on these and other occasions may inadvertently see the contents of e-mail messages. Therefore, there should be no expectation of privacy by users of the district e-mail system.

District network personnel (such as "postmasters") shall have the right to inspect e-mail when re-routing or disposing of otherwise undeliverable e-mail. This exception is limited to the least invasive level of inspection required to perform such duties. Re-routed mail normally should be accompanied by notification to the recipient that the e-mail has been inspected for such purposes.

#### 5. Access

Access to the Glenbrook High School District 225 e-mail system is a privilege that may be wholly or partially restricted by the district with or without prior notice. The district shall permit inspection, monitoring, or disclosure of e-mail with the approval of the superintendent or his designee, in the following situations:

- a. When permitted or required by, and consistent with, law;
- b. When reliable information indicates that violation of law or of district policies may have occurred;
- c. In circumstances where failure to act may result in significant bodily harm, property loss or damage, loss of evidence of one or more violations of law or of district policies, or liability to the district or to members of the Glenbrook High School District 225 community;
- d. In circumstances where failure to act could seriously hamper the ability of the district to function administratively or to meet its teaching obligations; or
- e. In any circumstance related to a pending investigation.

Employees shall comply with district requests for copies of e-mail records that pertain to the business of the district, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the district. When the contents of e-mail must be inspected, monitored, or disclosed, the superintendent or his designee must authorize such actions in advance and in writing.

In emergency circumstances, the least invasive perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must thereafter be sought as soon as reasonably possible. The superintendent or designee shall, at the earliest possible opportunity, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

Any inspection or disclosure of e-mail shall be in full compliance with the law. This has particular significance for e-mail residing on computers not owned or housed by the district. Advice of counsel should be sought prior to any action taken under such circumstances.

Failure to obtain an e-mail holder's consent prior to inspection, monitoring or disclosure of e-mail records shall not create any liability for the district.

#### 6. Archiving and Retention

##### a. Limitations and Automatic Purging

The district maintains central or distributed e-mail archives of all electronic mail sent from or received in users' mail accounts. E-mail is backed up to assure system integrity and reliability; e.g., to be able to restore damaged message databases, as well as retrieval. Administrators of the district e-mail service are not required to retrieve e-mails from such back-up facilities upon a user's request.

Except as otherwise set forth here, the district's electronic messaging system is intended as a communication system, as well as a record archive system. E-mail users should be aware that, due to hard disk space considerations on the district's message servers, specific maintenance procedures and mailbox size limitations (including e-mail attachments) will be implemented to ensure proper functioning of the e-mail system. Currently, messages in the user's mail account trashcan (deleted, but not purged) are subject to automatically be purged by the system. Users will be notified if server conditions warrant further automatically scheduled system maintenance that may affect the number or size of messages users may retain.

b. E-mail as a "Public Record"

The district is a public body governed by the *Illinois Local Records Act*, *Illinois School Student Records Act*, *Illinois Freedom of Information Act*, and the *Family Educational Rights and Privacy Act*. E-mails may contain information required to be retained in the official records of the district. Also, in certain circumstances, the district may be legally compelled to disclose e-mails to parents, government authorities, the public, or in the context of litigation. For retention purposes under these laws, e-mails are treated in the same manner as paper documents.

c. E-mail Retention

E-mails that meet the definition of a public record must be retained in accordance with the district's records retention schedule pursuant to the *Illinois Local Records Act*.

E-mails that meet the definition of a school student record must be retained in accordance with the *Illinois School Student Records Act*. Temporary student records must be kept for at least five (5) years after the student has transferred, graduated or permanently withdrawn from the district. Permanent student records must be kept for at least sixty (60) years after the student has transferred, graduated or permanently withdrawn from the district.

The following are acceptable methods for retaining e-mails. The district shall determine which method(s) it will use for a given record:

- (1) Print the e-mail and store the hard copy in the relevant subject matter file as would be done with any other hard copy public record;
- (2) Convert the e-mail into a Word or PDF document and store it in a file folder according to its content on the district's network;
- (3) Convert the e-mail into a microfilm or similar format (the district must comply with the *Local Records Act*, the *Filmed Records Certification Act*, and the *Filmed Records Destruction Act* if this method is used); or
- (4) Save the e-mail in the district's electronic document management system.

6. Archiving and Retention (continued)

d. Litigation Hold

All e-mails, without regard to whether they meet the definition of public and/or student records, must be retained when users receive notice of a litigation hold. The Superintendent or his/her designee will immediately inform users whenever e-mails must be preserved because of prospective, threatened or pending litigation (a "litigation hold"). Such notice immediately suspends the deletion and/or purging of all e-mails that may be relevant to the potential or pending litigation. The Superintendent or his/her designee will designate the district staff members responsible for gathering the e-mails that may be subject to the litigation hold.

e. Destruction of E-mails

The district's records custodian is responsible for disposing of the e-mails that are public records according to the records retention schedule and pursuant to the requirements of the Illinois Local Records Commission. In order to ensure compliance with such requirements, users are prohibited from deleting, purging and/or destroying e-mails that constitute public records. Users may not remove, "wipe" or erase the contents in their mail accounts or the e-mail software from their computers.

Destroying public records prior to approval for destruction will be considered tampering with official records. It is a Class 4 felony to knowingly tamper with records (720 ILCS 5/32-8).

7. Violations

Violations of this Board Policy governing the use of the Glenbrook High School Electronic Messaging Service may result in restriction of access to district information technology resources. In addition, disciplinary action may be applicable pursuant to Section F of Board Policy 7220, Purpose and Use of Technology and Network Resources, or other relevant Board policies.

8. Computer Services Termination Procedure

Once an employee's affiliation with the district ends, e-mail and network accounts may at the superintendent's or designee's discretion be kept open for thirty (30) days, retained by the district, or deleted at the discretion of the superintendent or designee, unless prior arrangements have been made. If an employee is suspended or terminated, or if a violation of this policy may have been committed, the computer services accounts of the employee will be locked immediately. Information can be requested from locked accounts for a period of up to thirty (30) days, which may be denied by the superintendent or designee for good cause. After this time the e-mail and network accounts may be deleted.

Revised: September 5, 1995  
Revised: May 29, 2001  
Revised: July 28, 2003  
Revised: September 12, 2005  
Revised: August 10, 2009  
Revised: August 8, 2011