Glenbrook High School District #225

BOARD POLICY: **ANNUAL BUDGET** **4010**

Section A

The superintendent or ~~his~~ designee shall prepare a tentative budget each year consistent with the district's mission and belief statement. ~~The process for developing the budget shall be approved by the Board of Education no later than it's first meeting in November and shall be substantially in the form of Exhibit A~~.

Section B

The superintendent or ~~his~~ designee shall utilize the following guidelines in developing the budget unless otherwise modified by the Board of Education:

1. Fund balance is the difference between assets and liabilities reported in a governmental fund. Fund balance measures the net current financial resources available to finance expenditures of future periods. Fund balance reporting will be in accordance with the most recent authoritative pronouncements and may include the following categories:

   a. Nonspendable: Includes amounts that are not in a spendable form. This would include, but is not limited to, inventory, prepayments and non-current receivables.

   b. Restricted: Includes amounts that can only be spent for specific purposes stipulated by external resource providers, law, regulation or contractual agreement. This would include, but is not limited to, bonded capital project funds and debt service funds.

   c. Committed: Includes amounts that are committed for a specific purpose by formal action of the Board of Education. Creation, amendment or modification to committed fund balance must also be approved by formal action of the Board by the end of the current fiscal year. Committed fund balance does not lapse at year end.

   d. Assigned: Includes amounts that are intended by the district to be used for specific purposes. Assigned fund balance represents amounts that are not restricted or committed. The Board of Education authorizes the assistant superintendent for business affairs to determine the assigned fund balance(s) on an annual basis. Assigned fund balance does not lapse at year end.

   e. Unassigned: Includes any remaining fund balance. The unassigned general fund balance may only be appropriated by resolution of the Board of Education.

   For purposes of fund balance classification, expenditures are to be spent first from Restricted Fund Balance (when appropriate), followed in order by Committed Fund Balance, Assigned Fund Balance and lastly, Unassigned Fund Balance.

Section B – (continued)

~~a.~~ 2. ~~Unrestricted~~ Unassigned reserves in the operating funds shall be maintained at a level equal to ~~approximately~~ not less than 33% of the next year's projected operating budget. (The operating budget is ~~composed~~ comprised of the education, food service, operation and maintenance, transportation, IMRF and working cash funds, and any other fund as may be required by State law.)

~~b.~~ 3. The budget shall first provide for staff and operating expenses to meet projected changes in student enrollment and mandated programs.

~~c.~~ 4. The budget shall reflect the Board of Education's desire to maintain the overall tax rate of the district when possible.

~~d.~~ 5. The budget shall reflect the Board of Education's desire to not increase the overall indebtedness of the district.

~~e.~~ 6. The budget shall reflect the Board of Education's desire to maintain safe and operationally sound facilities.

~~f.~~ 7. The budget shall anticipate compliance with all applicable governmental and legal obligations of the district.

~~g.~~ 8. The budget shall include a reasonable contingency for variable and unanticipated costs.

~~h.~~ 9. The administrative team shall in connection with the preliminary budget identify potential efficiencies from interbuilding, interdepartmental and district wide coordination or from building or district program or other organizational restructuring initiatives.

Section C

A draft of the Budget shall be presented to the Board of Education no later than the first regularly scheduled meeting in May supported by additional reports or analysis requested by the Board. A tentative budget shall be presented to the Board of Education for approval not later than its second regularly scheduled meeting in July. After tentative approval, the budget shall be made available for public inspection for no less than 30 days.

Section D

Final adoption of the budget shall take place at the next regularly scheduled Board Meeting following a public hearing posted and held in accordance with ~~s~~State ~~statute~~ law. Final approval shall take place no later than September 30.

Section E

Each fund shall include a contingency line item as established by the Board.

Section F

Any modifications to the ~~draft~~ tentative budget other than for changes in personnel costs and grant programs already approved by the Board of Education shall not be included in future iterations of the budget unless approved by the Board.

Section G

Transfers may be made between various budget line items in any fund not exceeding the aggregate of ten (10) percent of the total of such funds as set forth in the budget. The Board of Education shall be advised of all transfers ~~on a quarterly~~ on not less than an annual basis.

Section H

The Board of Education may amend the budget at anytime during the fiscal year by the same procedures provided for in its original adoption and in accordance with State law.

Approved: May 21, 1973
Revised: October 28, 1996
Revised: April 8, 2002
Revised:

BOARD POLICY: **PURPOSE AND USE OF TECHNOLOGY AND NETWORK RESOURCES 7220**

Section A - Introduction

It shall be the policy of the Board of Education of District 225 to encourage and facilitate communication and the exchange of ideas and information in pursuit of the district's curricular, instructional, technical, research, articulation and safety goals. The district also supports the use of technology as a tool for the efficient and effective management of the district's resources and affairs. Except for Section H – Children's Internet Protection Act (CIPA) Compliance, the provisions of this Policy shall apply to the use of technology by District employees or by students, whether provided by the District or self-provided~~,~~ (including hardware, software, and Internet access), in a Glenbrook school building, on school grounds, and at or in relation to a school-sponsored activity at any location in any manner that would otherwise violate this Policy.

Section B - Purpose of the District's ~~Computer~~ Technology and Network Resources

Glenbrook High School ~~computer~~ technology and network resources are for the use of authorized Glenbrook employees (including certain designated independent contractors and consultants), students and affiliated organizations. ~~The computers~~ District technology devices and the network, including any non-Glenbrook technology device, computer or network resource to which Glenbrook may be attached (e.g. Internet), are intended to provide authorized users with appropriate equipment and software to accomplish their district-authorized missions and to provide access to both local and worldwide ~~computer and network~~ electronic resources. ~~The systems~~ District technology and network resources and systems are intended for academic and administrative purposes only, as more fully described in Section C below.

The systems are not intended to be used for non-academic or non-administrative functions, or for personal or recreational use, which include, but shall not be limited to, illegal, commercial, political, religious or ~~personal~~ entertainment purposes, as more fully described in Section D below.

Section C - Acceptable Uses of Technology and Network Resources

Acceptable uses of technology and network resources include, but are not necessarily limited to, the following:

1. Curricular, instructional, co-curricular, and school-related extra-curricular activities or in support of such activities,

2. Research consistent with the goals and purposes of the district,

3. Communication among students, faculty, staff, and the local and global communities for academic or administrative purposes,

4. Development and implementation of curriculum,

5. Professional development of staff members,

6. Administrative or managerial record keeping, data access or research.

Section D - Unacceptable Uses of Technology and Network Resources

Unacceptable uses of technology and network resources include, but are not necessarily limited to, the following. Users may not:

1 Participate in, promote or facilitate any activity which is in violation of U.S. law, State or local law or Glenbrook Board Policy, or which will result in additional unplanned or unauthorized cost to the district as a consequence of network usage.

2. Interfere with, damage, modify or gain access to, in an unauthorized manner or disrupt computer or network users, services, data or equipment.

3. Participate in the acquisition, creation, or distribution of materials that are libelous, obscene, pornographic, promote the use of violence, contain personally embarrassing or private information unrelated to any proper educational or public purpose, contain defamatory or untrue statements which may damage ~~damaging~~ the reputation of any student or staff member, or contain abusive, harassing, or prejudicial content.

4. Participate in the acquisition, creation or distribution of advertising, computer "worms" or "viruses," "chain-letters," "spam" or other messages/files which could cause congestion, interference or failure of the system or any computing equipment, whether attached to the ~~D~~district's system or otherwise.

5. Make unauthorized entry to any computer, network, file, database, or communications device regardless of who may own, operate or supervise same and whether or not a change of data or software occurs.

6. Reveal personal account and/or password information.

7. Alter, damage or destroy any cabling, hardware, or software; ~~nor~~ or make unauthorized changes to district data.

8. Access, use or possess, distribute or disseminate unauthorized or illegally obtained hardware, software or data.

9. Engage in any activity that does not conform to the intended purposes of the network, including, but not limited to, illegal, commercial, political, religious, recreational or entertainment purposes.

10. Use technology and/or network resources or data for the purposes of academic dishonesty.

Section E - User Training

Employees and students using Glenbrook technology and network resources shall successfully complete an appropriate training program as prescribed by the District before being allowed to access the system. Depending upon the needs of the user, training may include, but shall not be limited to, login and logout procedures, access and use of various computer programs and/or network services, and instruction regarding security of accounts and passwords, copyright laws, computer ethics and network etiquette. Users are responsible for reporting any violations of this policy to an administrator.

Students and their parents/guardians will be informed as the students initially enroll in the district through the Glenbrook High Schools Technology Device and Network Use Students Rights and Responsibilities form and shall agree to be bound by the purpose of the network, how it is to be used, the need for mandatory instruction and the possible ramifications of inappropriate use as set forth in this policy and other Board Policies and Procedures, ~~or~~ and the Student/Parent Handbooks. Students and/or parents failing or refusing to agree to be bound by this policy shall be prohibited from using district hardware, software or network resources; however such students and/or parents shall remain subject to applicable Board Policies and Procedures related to the use of any non-Glenbrook and/or self-provided technology device, computer or network resource in a Glenbrook school building, on school grounds, and at or in relation to a school-sponsored activity at any location in any manner that would otherwise violate Board Policies and Procedures.

Section F - Disciplinary Action

1. Any student who is determined by the principal or designee to be in violation of this policy may have his/her network privileges suspended or canceled, or may be prohibited from possessing ~~student~~ self-provided technology devices in school buildings, on school grounds, and at or in relation to school-sponsored activities at any location. In addition, the student may be considered guilty of gross disobedience or misconduct and subject to additional disciplinary action by the administration and/or Board of Education. Such action may include, but is not limited to, suspension and/or expulsion from school.

2. Any employee who is determined by the principal or designee to be in violation of this policy may have their network privileges suspended or canceled. In addition, the employee may be subject to additional disciplinary action by the administration and/or Board of Education and may be required to provide user credentials for any user-based technologies or networks. Action by the Board of Education may include, but is not limited to, suspension with, or without pay, and/or termination of employment.

3. Cases involving suspected or alleged criminal acts will be referred to appropriate law enforcement agencies.

Section G - Termination of Authorized Use

The Board of Education recognizes the need for secure computing and networking facilities and authorizes the administration to terminate network/computer access when said access is no longer needed. Reasons for terminating the authorized use by an individual--student or employee--may include, but shall not be limited to the following:

1. A student is no longer enrolled at Glenbrook due to graduation, transfer to another school, dropping out of school, expulsion, death, ~~etc.~~ or other reason.

2. A student attends an educational facility outside of the Glenbrook district full-time but is still technically enrolled as a District 225 student.

3. A staff member is no longer employed at or is on leave from Glenbrook due to leave of absence, retirement, resignation, termination, death, etc.

4. Disciplinary reasons or violation of this policy.

5. Such other cause as the superintendent or chief technology officer determines in the exercise of reasonable discretion is necessary to secure the network operations, functionality and compliance with Board Policy pending further action in any disciplinary matter and pending finalization of such disciplinary determination or completion of any investigation.

6. Written revocation of consent by the student's parent or guardian.

Section H – Children's Internet Protection Act (CIPA) Compliance

1. Philosophy

   The district's philosophy and vision is to treat students as responsible young adults, and faculty and staff members as professionals. To prepare students to make wise choices, the district will educate them about responsible use of the Internet and the World Wide Web and hold high expectations of conduct in connection with their usage of this resource.

2. Children's Internet Protection Act (CIPA)

   It is the intent of the district to fulfill the requirements of CIPA. To accomplish this, Glenbrook High Schools will undertake actions intended to protect network users from web pages containing material that is illegal for minors, including, but not limited to, pornography. The district will take steps to address the safety and security of minors when using electronic mail and other forms of direct electronic communications. The district will take actions to prohibit unauthorized access, including "hacking," and other unlawful activities by network users; and prohibit the unauthorized disclosure, use, and dissemination of personal information regarding minors. Glenbrook High School District 225 will make reasonable efforts to block access to frivolous (non-educational) web sites that its administrators determine have a realistic potential to seriously impair or endanger the performance of the network, or otherwise result in a disruption of the school learning environment. Students will be permitted to access educational web sites and chat rooms consistent with this policy.

3. Educating Users

   a. The district will provide instruction for users in proper research techniques for various sources, including online subscription research products available through school or public libraries, printed materials, and Internet sources in addition to general search engine use.

   b. The district will inform users of the expectations for responsible network use and obtain their signatures, or in the case of students under the age of eighteen (18), the signature of their parent or guardian in agreement to the standards listed.

   c. The school will provide Internet safety instruction during each year of a student's high school career as required by State ~~Code~~ law.

4. District Responsibilities

   The district will be responsible for the following actions in order to comply with CIPA:

   a. Implement a content filter for known pornographic sites including visual images. A content filter contains a list of web sites to be blocked from Glenbrook user access.

   b. Impose a blocking list for specific websites intended for ~~whose~~ non-educational use or which use degrades network response times.

   c. Supervise student use of the Internet as thoroughly as possible.

   d. Make reasonable efforts to ~~M~~monitor Internet web site traffic for patterns of usage that could indicate inappropriate network usage. If questionable material is accessed repeatedly, the chief technology officer will be alerted to the situation and will forward the information to the superintendent who shall act as is deemed appropriate.

   e. When a network use violation occurs by a student, the principal or designee will be given all details available in order to take appropriate action in accordance with Section F of this policy.

   f. When a network use violation occurs by a faculty or staff member, the superintendent, assistant superintendent for human resources, building principal, and instructional supervisor will be given all details available. Appropriate action will be taken in accordance with Section F of this policy.

5. Blocking List

   The blocking list determines what is filtered. The blocking list will contain, at a minimum:

   a. Known sites of material, illegal for minors, including, without limitation, pornography.

   b. Non-educational sites that seriously degrade performance of the network or pose network intrusion risks.

   c. Sites which will result in ~~additional~~ unplanned or unauthorized cost to the district.

   As the district learns of additional sites that should be blocked in the categories listed above, the chief technology officer will direct necessary and appropriate changes to the blocking list. If temporary and/or immediate changes to the Blocking List are requested for educational purposes, the chief technology officer, ~~the network manager, or other~~ the superintendent or authorized designees must approve them.

   If the District Administrative Team (ATM) requests changes in the categories included on the blocking list, those changes must be approved by the Board of Education.

DISCLAIMER. In compliance with CIPA, the district endeavors to protect Glenbrook network users from web pages containing material that is illegal or inappropriate for minors, including, but not limited to, pornography. The district also endeavors to address the safety and security of minors when using electronic mail and other forms of direct electronic communications through the Glenbrook network. However, the use of ~~employee~~ self-provided ~~and student-provided~~ technology to access the Internet network cannot be subjected to measures used by the district such as content filters, blocking lists, or district monitoring of Internet web site traffic for patterns of usage that could indicate inappropriate network usage. Accordingly, employees and students who provide their own technology and/or access to the Internet shall assume any risk associated therewith. The district expressly disclaims any responsibility for imposing content filters, blocking lists or monitoring of employee or student-provided technology and/or devices.

Section I - Dissemination to Students and Employees

1. All employees will be given a copy of the Board Policy for their signature. New employees will be given a copy of the Board Policy for signature at the time of signing their respective employment contract. The assistant superintendent for human resources and chief technology officer will coordinate the process.

2. Excerpts of this policy will be included in the Student/Parent Handbook for each school. Upon initially enrolling in the district, students and parents will be asked to sign ~~a document~~ the Glenbrook High Schools Technology Device and Network Use Student Rights and Responsibilities form giving permission for network and Internet access and agreeing to the provisions of this policy. If at any time a parent determines that their child should not be allowed access to the Internet, they are to submit a written request to discontinue services to the assistant principal for student services. Students or parents failing or refusing to be bound by this policy shall be prohibited from using District hardware, software or network resources.

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, ~~or~~ 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.

As a convenience, employees may "advertise" items of a one-time, short-term nature such as concert or event tickets that they cannot personally use. To do this, send an e-mail to "AD". "AD" is a special e-mail account that everyone in the district can read. All users can send messages to "AD". All users can read messages in that account by setting up a proxy, and everyone can reply to messages there. All postings in the "AD" mailbox will automatically be purged after 14 days. Users should not send "advertisement" e-mails to building or district e-mail groups directly.

3. Efficiency

Attachments and html-formatted messages are usually larger than text messages. Users should consider this fact due to the size limitation on individual mailboxes. Whenever possible, avoid attachments by putting the information in the body of the e-mail.

4. 3. Confidentiality

The security and confidentiality of electronic mail cannot be guaranteed and all such 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.

The nature of e-mail makes it less private than users may anticipate. For example, e-mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an e-mail posted on an electronic bulletin board or list serve intended only for the originator of the message may be distributed to all subscribers to the list serve. Even after a user deletes an e-mail, it may persist on backup facilities, and thus be subject to disclosure.

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 personal any e-mail resident on district facilities. Users, therefore, should exercise extreme caution in using e-mail to communicate confidential or sensitive matters.

~~5.~~ 4. Exceptions

~~Users should be aware that,~~ ~~d~~During the performance of their duties, district system administrators ~~need~~ 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.

District network personnel (such as "postmasters") ~~may need~~ 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.

~~6.~~ 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, ~~significant~~ property loss or damage, loss of ~~significant~~ evidence of one or more violations of law or of district policies, or ~~significant~~ 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 ~~are expected to~~ shall comply with district requests for copies of e-mail records ~~in their possession~~ 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 ~~then~~ thereafter be sought ~~without delay~~ 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 ~~except and unless such action was a willful violation of Board Policy and done for an improper purpose and in bad faith~~.

~~7.~~ 6. Archiving and Retention

a. Limitations and Automatic Purging

The district ~~does not~~ maintains central or distributed e-mail archives of all electronic mail sent from or received in users' mail accounts. E-mail is ~~normally~~ backed up to assure system integrity and reliability; e.g., to be able to restore damaged message databases, ~~not to provide for future~~ 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, ~~not~~ 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*. ~~If an e-mail that must be retained is not otherwise described in the records retention schedule, it will be retained for one calendar year.~~

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.

~~7.~~ 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 ~~a~~ prospective, threatened or pending 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).

~~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.

~~9.~~ 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 ~~and then will be~~ deleted at the discretion of the superintendent or designee, unless prior arrangements have been made ~~with the district network technicians or the coordinator of instructional technology~~. 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:

Glenbrook High Schools ~~Computer~~ Technology Device and Network Use
Employee Rights and Responsibilities

Employee Privileges

Glenbrook employees have the privilege to use Glenbrook computers and electronic devices in order to facilitate educational growth in technology skills, information gathering skills, and communication skills, and to perform administrative tasks. These computers and electronic devices may provide access to the Internet. Employees have the privilege to use any licensed district standard software.

Employee Responsibilities

Only those employees with prior experience and/or instruction shall be authorized to use the Glenbrook network and Internet access. The employee will not allow others to use his/her computer account, nor will he/she disclose his/her passwords to anyone. Employees may not alter any Glenbrook network address or identifiers or use false identities. Employees may not copy Glenbrook software from district devices, violate copyright laws, destroy or damage another person's files or messages, copy other people's work, or attempt unauthorized access to networks in or out of the building. They may not make unauthorized entry, interfere with, or disrupt any computer, network, service or equipment, regardless of who may own, operate or supervise it. The employee has the responsibility to report all violations of privacy or of this policy pertaining to his/her computer accounts to the coordinator of instructional technology or chief technology officer.

Faculty and staff have a professional responsibility to ensure appropriate use of technology by students. An adult will monitor all student Internet use accessed by district and student-provided technology as thoroughly as possible.

The employee is responsible for honoring copyright laws when using electronic media, including but not limited to software, original art work, video, and Internet copyrighted material.

The employee is responsible for all data communications originating from his/her account. Furthermore, the employee is responsible for making sure all communications originating from the Glenbrook network by him/her do not contain pornographic material, inappropriate content ~~information~~, inappropriate language, data that is in violation of this policy, or files that are potentially dangerous to the integrity of the network infrastructure. Solicitation of such materials is also prohibited.

The intent of Glenbrook's Internet connection is for education use, and not for individual profit. Each employee has the responsibility not to use the network for wasteful or frivolous purposes such as playing network games. No sites shall be accessed which will result in ~~additional~~ unplanned or unauthorized cost to the district.

All data communications sent or received through the Glenbrook network may be monitored by district network administrators and shall remain the property of the district.

Failure to comply with the "Purpose and Use of Technology and Network Resource" Policy may result in loss of computer privileges as well as other disciplinary action. The employee acknowledges that his/her choice to use employee-provided technology (including hardware, software, and Internet access) in any manner that would otherwise violate this Policy will subject the employee to discipline. The employee acknowledges his/her responsibility to comply with Board of Education Policy 7220, which is available at http://www.glenbrook225.org/board/policies/Documents/7220.pdf

District Responsibilities

The district will use reasonable efforts consistent with available budgetary approvals to provide current anti-virus software for workstations and servers, as well as e-mail servers. Users will receive instructions for maintaining secure passwords and access to their accounts. The district will implement Internet content filtering on the Glenbrook network according to Board Policy. The district will make reasonable efforts to maintain secure backups of file servers. The district will comply with all applicable laws relative to the privacy of employee and student information.

_____

I have read this document and the "Purpose and Use of Technology and Network Resources" Policy, and agree to abide by them. I will uphold my responsibilities as a user of Glenbrook High School computers and networks.

Printed Employee Name _____ Date _____
Employee Name _____ Date _____

Glenbrook High Schools ~~Computer~~ Technology Device and ~~Glenbrook~~ Network Use
Student Rights and Responsibilities

Student Privileges

Students have the privilege to use Glenbrook computer workstations in order to facilitate educational growth in technology skills, information gathering skills, and communication skills. These workstations may provide access to the Internet.

Student Responsibilities

In order for Glenbrook High Schools to provide sound educational opportunity via the network, each student needs to use the Glenbrook computer network system responsibly.

The student exercising his/her privilege to use the Glenbrook computer network system or ~~student~~ self-provided technology to access the Internet as an educational resource is responsible for all material received. Only those students with prior experience and/or instruction shall be authorized to use the Glenbrook computer network system to access the Internet. Students are responsible for not giving their Glenbrook computer account and password to anyone. Students may not alter any Glenbrook network address or identifiers or use false identities. Students may not copy Glenbrook software from ~~computers~~ district devices, violate copyright laws, destroy or damage another person's files or messages, copy other people's work, or attempt unauthorized access to networks in or out of the building. They may not make unauthorized entry, interfere with, or disrupt any computer, network, service or equipment, regardless of who may own, operate or supervise it.

Students are not allowed to access, use or possess pornographic material, inappropriate, harassing or offensive ~~text~~ content via e-mail or other means, or files deemed dangerous to the integrity of the Glenbrook High School network system. In addition, students may not access, use or possess unauthorized or illegally obtained hardware, software or data. The intent of Glenbrook's Internet connection is for educational use, and not for individual profit or recreational purposes that promote waste, fraud or abuse. No sites will be accessed that result in ~~additional~~ unplanned or unauthorized cost to the district.

If a student has been assigned a Glenbrook e-mail account, the student is responsible for reporting all violations of privacy or of this policy. Students are accountable for all mail received under their user accounts.

Students may not use the network or labs for wasteful or frivolous purposes. It is the student's responsibility to follow all computer lab rules and obey supervisors of all school labs, and follow the guidelines for acceptable use of electronic devices as established by the school administration.

The student acknowledges that his/her choice to use ~~student~~ self-provided technology (including hardware, software, and Internet access) in a Glenbrook school building, on school grounds, or at or in relation to a school-sponsored activity at any location that in any manner that would otherwise violate this Policy will subject the student to discipline. Such discipline may include confiscation of the ~~student~~ self-provided technology, loss of Glenbrook computer privileges, and other penalties and disciplinary actions up to and including suspension and expulsion.

The student acknowledges his/her responsibility to review and comply with the requirements set forth in Board of Education Policy 7220, "Purpose and Use of Technology and Network Resources" which is available at http://www.glenbrook225.org/board/policies/Documents/7220.pdf

District Responsibilities

The district will use reasonable efforts consistent with available budgetary approvals to provide current anti-virus software for workstations and servers and to maintain secure backups of file servers. Users will receive instructions for maintaining secure passwords and access to their accounts. The district will implement Internet content filtering on the Glenbrook network according to Board Policy and will comply with all applicable laws relative to the privacy of staff and student information.

I have read this document and the "Purpose and Use of Technology and Network Resources" Policy and agree to abide by them, and to uphold my responsibilities as a student user of Glenbrook High School computers and networks, and to uphold the same responsibilities as a condition of using ~~student~~ self-provided technology in a Glenbrook school building, on school grounds, or at a school-sponsored activity at any location.

Student Name _____ID Number _____ Date _____
Student Signature _____ School _____
Parent Signature _____ Date _____

Glenbrook High Schools
Student Electronic Messaging Accounts

I have read **Section J - Use of the Glenbrook Electronic Messaging System** (from Board of Education Policy 7220) and agree to abide by it, and to uphold my responsibilities as a student user of Glenbrook High School computers and networks.

Student Name _____ ID Number _____ Date _____

Student Signature _____ School _____

Parent Signature _____ Date _____