Hazleton Area School District
Employee Acceptable Use Agreement Form

Employees of the Hazleton Area School District may access the Internet or email for educational or work-related purposes at any time that it does not interfere with the performance of other responsibilities by the employee.

All users must have a signed copy of this form on file with the school district Technology Department prior to using the Internet.

Internet use is a privilege and inappropriate use may result in cancellation of Internet privileges and/or other disciplinary actions. All employees must abide by the following rules:

1. I will use the district's Internet access for constructive educational and work-related purposes only.
2. I will not access sites that contain illegal, defamatory, pornographic, or otherwise offensive material.
3. I will not circumvent or attempt to circumvent the district's Internet filtering measures.
4. I will report to one (1) of my superiors any such offensive information contained in any file that I might uncover within the district's network.
5. I will observe the district rules and laws regarding copyright (Policy 814) and plagiarism.
6. I will never post on any website another person's home address, telephone number or any other such personal information.
7. I agree to follow any other rules for Internet and local network use that the district establishes, including but not limited to the following HASD polices, each of which are available for my review on HASD's publicly accessible website.
    - 815 Acceptable Use of Internet, Computers and Network Resources
    - 815.1 Use of School-Owned Laptop Computers
    - 815.2 Computer-Related Technology
    - 815.3 Software Licensing, Approval and Installation
    - 815.4 Technology Requests
    - 815.5 Social Media
    - 816 Email

Employee Certification Form

I have read and understand the district's Internet Acceptable Use of Internet, Computers and Network Resources Policy 815 and Faculty Email Policy 816 and the information provided on this form. I understand and will abide by the conditions and rules set forth herein. Should I fail to follow explicitly the rules enumerated above, my access privileges may be revoked and disciplinary action may be taken, up to and including termination of my employment by the district. I understand that appropriate legal action will be taken by the district when warranted, and I further understand that I will be held responsible for any costs incurred by my inappropriate use of the Internet. I am aware that law enforcement agencies must be consulted if violations of these conditions and rules may constitute a criminal offense.

_____ _____

Employee Date

_____ _____

Printed Name School

Book	Policy Manual
Section	800 Operations
Title	Computer-Related Technology
Code	815.2
Status	Active
Adopted	August 18, 2011
Last Revised	April 28, 2022

Purpose

The Board shall provide resources to support the use of computers, Internet and network resources in the district's instructional and operational programs.

Guidelines

Computer-Related Technology Purchases

Building-Based Technology Purchases –

All computer-related technology purchases must be initially approved by the building principal and must promote the goals of the district's comprehensive plan.

The district's technology department shall evaluate all building-based technology purchases to ensure that the equipment being purchased maintains the integrity of the district's network. The technology department shall determine the appropriate equipment bid prices and shall develop specifications if items are to be competitively bid, in accordance with Board policy and applicable law and regulations.[1]

The Director of Technology, Business Manager, and Superintendent shall sign off on all building-based technology purchase orders.[2]

Administrative Technology Purchases –

The district's technology department shall evaluate all administrative technology purchases to ensure that the equipment being purchased maintains the integrity of the district's network. The technology department shall determine the appropriate equipment bid prices and shall develop specifications if items are to be competitively bid, in accordance with Board policy and applicable law and regulations.[1]

The Director of Technology, Business Manager, and Superintendent shall sign off on all administrative technology purchase orders.[2]

Installation of Computer-Related Equipment

The technology department shall assume responsibility for the installation of all computer-related equipment. If a contracted vendor is installing equipment in the district, the technology department shall assure that all contracted work has been completed to specifications and is fully operational prior to payment to the contractor. All technology-related contracts in excess of $10,000 shall follow reporting requirements. The Director of Technology shall submit a short narrative to the Superintendent and Business Manager detailing the contract's closeout prior to making final payment.

Ensuring the Completion of Technology-Related Training

The specific program director or administrator initiating the deployment of a new technology product shall be responsible for ensuring that the contracted computer training is followed as per the negotiated contract.

Legal
1. Pol. 610
2. Pol. 611
24 P.S. 510
Pol. 815

Book	Policy Manual
Section	800 Operations
Title	Use of School-Owned Laptop Computers and Associated Technology
Code	815.1
Status	Active
Adopted	August 18, 2011
Last Revised	April 28, 2022

Authority

The Board authorizes district-owned laptop or tablet computers and associated technology to be used off school property if said equipment is being used by a district employee as a tool to enhance work performance and improve the instructional process, or being used by a student as a tool or resource to enhance instruction. If equipment is assigned to a specific individual, that individual shall be fully liable for loss of equipment and excessive damage during the period of use. In the event of loss or damage, the responsible person will be required to compensate the district for the cost of repair or replacement. This equipment shall be used only by authorized individuals.

Delegation of Responsibility

The building principal or specific program director may grant the use of equipment after school, during the summer, or as otherwise needed. An authorization form must be completed, signed, and returned to the School Office prior to the removal of any equipment from school grounds. Under no circumstances may a District-owned laptop or tablet computer be used for personal purposes.

The district's Office of Asset Inventory and Office of Security Operations shall conduct a semi-annual inspection of all equipment. A random inspection of the equipment may be conducted anytime at the district's discretion.

The user shall be responsible for loss of equipment as a result of fire, theft, excessive damage, etc., not covered by the district's equipment maintenance contract. The replacement cost shall be determined based on the present market value of the item, not to exceed the original purchase price of the item.

Issues related to malfunction or damage to equipment covered under the district's equipment maintenance policy must be reported to the appropriate department within a timely manner, not to exceed one (1) week or five (5) working days.

Legal
24 P.S. 510
Pol. 815

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Code	815
Status	Active
Adopted	August 18, 2011
Last Revised	April 28, 2022

Purpose

The Board supports use of the computers, Internet and other network resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research, and collaboration.

The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

For instructional purposes, the use of the Internet and network facilities shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Definitions

The term child pornography is defined under both federal and state law.

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:[22]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.[23]

The term harmful to minors is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:[2][3]

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and

3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[24]

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

Obscene - any material or performance, if:[24]

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and

3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure - a specific technology that blocks or filters Internet access to:

- visual depictions that are known to be obscene, child pornography, or harmful to minors [3]
- any areas on the Internet that are known to have a serious potential to lead to physical, psychological, or emotional harm to minors

Authority

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet, including but not limited to data that is graphic, video, audio, text, etc.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.[4][5][6]

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:[3]

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.[7][8][9][10][11]
5. Bullying.[12]
6. Terroristic.[13]

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or

online server blocking and filtering. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.[2][3][14]

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.[14]

Delegation of Responsibility

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[14]

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and may use tracking systems to track and recover lost or stolen equipment.[16]

Student user agreements shall also be signed by a parent/guardian.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[2][3][19]

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[3]

1. Interaction with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.[12][18]

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Access to Information

Information is no longer restricted to books, libraries, and broadcast media. The World Wide Web is the most up-to-date source of information on every conceivable topic. Countless organizations globally contribute to its content. Students and teachers may use this rich source of global information regularly in their classrooms. New skills are required – the skills of scanning, assessing for relevance and selecting from the vast amount of information retrieved. District teachers and staff shall assist students in developing skills necessary to use this resource responsibly and in accordance with Board policy and administrative regulations.

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[3][19]

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

3. Prevention of unauthorized online access, including "hacking" and other unlawful activities.

4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of minors' access to materials harmful to them.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.

2. Commercial or for-profit purposes.

3. Nonwork or non-school related work.

4. Product advertisement or political lobbying.

5. Bullying/Cyberbullying.[12][18]

6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[20]

9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

10. Inappropriate language or profanity.

11. Transmission of material likely to be offensive or objectionable to recipients.

12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.

13. Impersonation of another user, anonymity, and pseudonyms.

14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.[21]

15. Loading or using of unauthorized games, programs, files, or other electronic media.

16. Disruption of the work of other users.

17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

18. Accessing the Internet, district computers or other network resources without authorization.

19. Disabling or bypassing the Internet blocking/filtering software without authorization.

20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

21. Use of unauthorized chat rooms and/or other forms of direct electronic communication for noneducational purposes.

Security

System security is protected through the use of passwords and an Internet firewall, which will only allow access to authorized users. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.[21][25]

District Website

The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. The cost of damages will include, but is not limited to, hardware replacement costs, legal costs, and labor costs to identify and remedy the damages.[14]

Illegal use of the network; intentional deletion or damage to files or data belonging to others; uploading, downloading, or creating computer viruses; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. [4][5][6]

Legal
2. 20 U.S.C. 6777
3. 47 U.S.C. 254
4. Pol. 218
5. Pol. 233
6. Pol. 317
7. Pol. 103
8. Pol. 103.1
9. Pol. 104
10. Pol. 248
11. Pol. 348
12. Pol. 249
13. Pol. 218.2
14. 24 P.S. 4604
15. 24 P.S. 4610
16. Pol. 815.1
18. 24 P.S. 1303.1-A
19. 47 CFR 54.520
20. Pol. 237
21. Pol. 814
22. 18 U.S.C. 2256

23. 18 Pa. C.S.A. 6312
24. 18 Pa. C.S.A. 5903
25. 17 U.S.C. 101 et seq
24 P.S. 4601 et seq
Pol. 220
Pol. 815.2
Pol. 815.3
Pol. 815.4
Pol. 816

Book	Policy Manual
Section	800 Operations
Title	Software Licensing, Approval and Installation
Code	815.3
Status	Active
Adopted	August 18, 2011
Last Revised	April 28, 2022

Purpose

The Board shall provide software resources to support the use of computers and network systems in the district's instructional and operational programs.

Guidelines

Software Records

For all purchased software, district staff shall submit the following information to the Technology Department:

1. Proof of Purchase - Copy of Purchase Order and/or Receipt, if available.
2. Original License. If no license is on file, one (1) license per purchase or quantity stated on receipt will be assumed.
3. Media, URL of download source, or online vendor confirmation number.
4. Completed Software Request Form.

Software Purchases

All software purchases shall first be approved by the building principal and the department chairperson to verify that the software being considered supports the curriculum or district operations. In addition, all software purchases shall be approved by the Technology Department to assure system compatibility and licensing requirements. Software will not be installed otherwise. Before selecting software, please review the attached list of Frequently Asked Questions. Approval may be obtained by sending the required information to the Technology Director.

Any software with a purchase price of fifty dollars ($50) or more per license should be fully tested to ensure compatibility with the Hazleton Area School District's network. Prior to purchasing multiple licenses of software in this category, employees shall submit a completed Software Request Form with minimum system requirements noted. In addition, employees shall purchase one (1) license, or obtain a demonstration copy of the product, and send it to the Technology Department for testing. If approved, software shall be returned for the purchase of multiple licenses.

Software Request Form

The purpose of the Software Request Form is to convey software needs to the Technology Department.

The Technology Department must evaluate all software purchased for compliance with the Hazleton Area School District's network. To ensure technical support and/or training, employees shall complete the Software Request Form and seek approval from the building principal, director and/or department chair.

Procedure for Software Installation

Before software may be purchased, employees shall:

1. Review the attached "Items to Consider When Purchasing Software FAQs" to ensure that the software will meet district needs and conform to district goals.

2. Complete a Software Request Form and submit the form to the building principal, departmental chair, and/or director, then forward to the Technology Department.

3. Receive the Software Request Form marked Approved.

Once approved, after purchase and prior to the software being installed on district computers, the following shall be sent to the Technology Director:

1. The original license agreement.

2. A copy of the Purchase Order, including software titles, vendor name and amount of licenses.

3. Media source and installation instructions.

4. A list of the school(s), room(s), and computer(s) in which the software shall be installed.

5. Employee name, department, and phone number.

All correspondence and coordination regarding software installation shall take place via email. Software shall not be installed without prior approval, proof of purchase, and original licensing. Questions shall be directed to the Technology Director.

Licensing Terms

Standard Licensing - One (1) piece of software to one (1) computer.

Site Licensing - One (1) piece of software to many machines.

Legal
24 P.S. 510
Pol. 814
Pol. 815

815 3-Attach.doc (45 KB)

Items To Consider When Purchasing Software FAQs

1. **Does the software directly correlate with the curriculum and meet or support standards?** There are thousands of programs vendors want you to buy. Consider only the best, with a direct purpose, focus, and targeting a direct curricular need.

2. **Will the vendor be in business next year?** Please choose a vendor with a history of successful business operations. New vendors should be avoided at first, no matter how innovative the product, due to how volatile and short term the industry tends to be.

3. **What warranty will be provided?** Software must have a warranty. Vendors that do not provide some sort of warranty for their product are to be avoided.

4. **Will the software integrate with other software used by the HASD Technology Department?** This is crucial. Although some software vendors may recommend new systems to run their software properly, such software should be avoided as it will result in significant additional costs and time on the HASD's support infrastructure.

6. **Will the software adapt to the HASD instructional systems standard?** Will the software integrate with the current systems and meet the guidelines for acceptable software in use at the district? If you are unsure of these questions, seek the assistance of the Technology Department to help you determine the answer.

7. **What flexibility will it provide?** The software should be "expandable" or easily reconfigured/updated to meet your future needs. It should also be able to meet projected needs/capabilities that you may have in the near future.

8. **Is the HASD current hardware compatible?** Our equipment should be able to run a very broad range of software; however, check with the vendor to ensure basic compatibility with the deployed hardware in the district.

9. **Will documentation provided be user friendly?** The software should come with solid, easy to read and understand manuals and help pages. Printed form is preferable over electronic format. Additionally, online web support is a plus.

10. **What training is offered?** Does the vendor provide on-site training or some other form of training? It is recommended by the Technology Department that any software vendor being considered should be able to provide some form of training, and that training resources be readily available.

11. **What other expenses will be incurred?** Consider the costs of additional hardware, hardware upgrades, training, licensing, ongoing maintenance and support contracts, and relicensing on a schedule prior to committing to a software product. These costs can sometimes be hidden, thus adding to the final cost for the product.

12. **Can the vendor provide modifications?** This is important if the software is "close" to meeting your needs and the vendor is acceptable under the HASD standards. The option, usually at some cost, of modifying a software program should be considered and the vendor should be questioned to ensure that modification is a possibility.

13. **Is there an upgrade planned in the near future?** If a vendor plans on a major software revision or upgrade in the near future, waiting for the next version may be something to consider. If the need is immediate, disclosure by the vendor should be made of what impact the upgrade or revision will have on training, usage, hardware requirements, and overall long-term cost.

14. **Is there a vendor help desk?** Typically, a help desk support option is the first and easiest step in acquiring support should a problem arise with a product. Make sure your vendor has adequate support available for their customers prior to any purchase.

15. **What is the vendor's reputation?** Any vendor considered by the HASD should have a good business and product reputation. Ask other users of the product and look for third party reviews to help establish the vendor's reputation prior to any purchase.

16. **How complex is the installation?** The Technology Department wishes to support all of its users in a timely fashion. Please ensure that the installation of the software is relatively standard. If not, please let the Technology Department know in advance if special actions or activities will be needed to install a particular software product. This will help the Technology Department prepare adequately and schedule accordingly.

17. **Will the vendor supply names of current users as references?** When reviewing the reputation and history of a vendor to determine their suitability for providing a product to the HASD, ask for a list of current users of the product. The vendor should provide this freely and without hassle. If the vendor does not provide this list, weigh their lack of cooperation accordingly.

18. **Is there a user support group(s)?** Determine if groups of users exist and how to contact them. These may range from simple online groups to complicated associations of users across the country. These are sometimes key points for acquiring support on difficult usage issues or problems, as well as good places to collect ideas for further integration of the product into your day-to-day operations.

19. **Grant money purchases:** Any software that is approved for purchase, but is using grant money must be able to cover the costs of licensing for a minimum of three (3) years.

Book	Policy Manual
Section	800 Operations
Title	Technology Requests
Code	815.4
Status	Active
Adopted	August 18, 2011
Last Revised	April 28, 2022

Purpose

The Board shall provide technical support resources to support the use of computers and network systems in the district's instructional and operational programs.

Guidelines

The following procedures shall be enforced by the Technology Department and specify the types of assistance provided by the Site Manager.

Prioritization of Technology Requests

1. Network down
2. Room unable to connect to network
3. Building-wide software issue
4. User account problem (network and email accounts)
5. Internet access problem
6. Classroom Instructional Technology problem
7. Computer problem
8. Network printer problem

All technology related issues must be reported via the district's help desk system. In the event of a building level technology emergency, the Building Administrator may contact the Technology Director via cell phone to report the issue immediately.

Each school's Site Manager shall email all repair/request issues to the district's help desk system. This information is automatically available to the Technology Department. To maintain efficiency, the Technology Department staff shall only address items listed on the help desk ticket. All building issues shall be appropriately scheduled for service.

The Site Manager shall serve as the building liaison with the Technology Department. All building level repairs, projects, inventory, and training requests must be requested

by the Site Manager. District employees may submit their own help desk tickets for individual of classroom technology issues.

Administrative computers, such as office, maintenance, security, library, guidance, and special education (non-classroom systems), shall require Technology Department assistance regarding troubleshooting. Set up of any new administrative users and email accounts must be communicated through the Site Manager to the Technology Department via help desk email.

The Site Manager shall assist with minor day-to-day issues such as network troubleshooting, printing, hardware, and software problems.

Any hardware moves shall require prior Technology Department approval. In addition, the proper Equipment Transfer slip must be completed and forwarded to the Technology Department.

The Site Manager shall coordinate professional development activities with the building planning team and the building principal.

Technology Department staff are the only personnel authorized to install software on the district network or district computers.

Any grant or scholastic achievement award projects that involve technology must be coordinated through the Technology Department prior to grant application or acceptance of the award.

Walk-in traffic to the Technology Department must be limited due to server security and scheduled projects.

If a Site Manager is not available and an individual would like to drop off equipment, it must be logged and scheduled the same as all other requests.

Legal
24 P.S. 510
Pol. 815
Pol. 815.2
Pol. 815.3

Book	Policy Manual
Section	800 Operations
Title	Social Media
Code	815.5
Status	Active
Adopted	March 29, 2012
Last Revised	April 28, 2022

Purpose

The Hazleton Area School District recognizes the prevalence of Social Networking in personal and professional communications. This policy addresses employees' use of such networks, including: personal websites, web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other kind of social media.

Student access to non-district approved personal websites, web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other kind of social media is prohibited when using any district device, district network, district Internet access, and at any time when the student is attending school for scheduled education.

The district takes no position on employees' decisions to participate in social media such as that described above, and is cognizant of the constitutional protections afforded to employees speaking as private citizens on matters of public concern. However, employees are reminded that they are professionals and are representatives of the district and the community in all aspects of their lives. At all times, including the course of communications via social media, employees should conduct themselves publicly in accordance with the responsibilities of public service. This policy is intended to assist the employee in making good decisions when communicating and obtaining information online in accordance with district policy.

The Superintendent, and/or designee, is hereby granted the authority to create and enforce additional administrative regulations, procedures, and rules to carry out the purpose of this Social Media policy. These administrative regulations, procedures, and rules may include, among other items, guidance in implementing and using school district-sponsored social media and other websites for educational purposes, upon request. This policy notwithstanding, users are always responsible for their own behavior when communicating via social media.

Users will be held accountable for the content of communications that are posted via social media sites, when appropriate. Users are responsible for complying with the school district's Acceptable Use policy and related guidelines addressing the use of social media. At no time may any user of the district network disrupt the learning

atmosphere, educational programs, school activities, and/or the rights of others via use of a social media site or other form of electronic communication.

Guidelines

Interaction with Students Through Blogs and Social Networking

Employees are required to maintain a professional relationship with their students at all times and are prohibited from becoming friends and/or communicating with students via personal accounts on social media networks. Further, employees should not engage students on either the employee's or the student's blog or social networking page regarding any other matter. Employees should not participate in student social networking group pages or utilize these pages to communicate with students in a personal capacity when they know or should have known that students are involved and participating.

Only school-sponsored websites, wikis, email addresses or other district-sponsored means should be utilized for communications with students and/or parents. In the event an employee receives a communication or request from a student or parent addressed to the employee's personal account, the employee should respond via other means that are district-sponsored.

If an employee wishes to establish a school-sponsored social media account, page, or other platform to address extra-curricular activities for purposes of scheduling and/or other administrative communications, they may submit a request in writing to the Hazleton Area School District Superintendent. Under no circumstances should employees be utilizing personal accounts for such purposes. This acknowledgement of a potential exception for communications with students via social media sites sponsored by the district is limited to circumstances unique to extra-curricular and co-curricular activities that require interaction between coaches and other district personnel with students whom they may not see during the course of the school day. This exception is not intended to apply to, or otherwise permit general, personal, or assignment-related communications between employees and students. Such communication should be occurring solely via district-sponsored means of communication, such as e-mail.

Identification and Authorship

The district encourages employees to be honest about their identity when utilizing social media. Tracking tools enable supposedly anonymous posts to be traced back to their authors. Employees should not pretend to be another person in order to pursue personal communications or agendas, and are prohibited from doing so when communicating about district matters of private or internal concern regarding the district, its staff, students or operations.

Employees are prohibited from acting as a spokesperson for the district or posting comments as a representative of the district without express consent. Any employee who chooses to identify him or herself as a district employee on any social media network or offers any comment on any topic related to the district, while on any social media network, is directed to include a disclaimer providing that follows:

"The views expressed [in the social media format] are mine alone and do not necessarily reflect the views of the Hazleton Area School District."

Monitoring and Liability

Employees should understand the public nature of the Internet and should understand that the district is free to view and monitor employees' public websites, blogs, or other public internet communications at any time, without consent from the author of such communications. Furthermore, as representatives of the district, employees are reminded that students, parents, and other partners of the district community are able to view any public communication or private social media communication made accessible to them by district employees. It is the responsibility of all employees and/or users of social media to carefully consider their behavior and what they place on line when communicating with, or "friending", any individual. Information placed in social media, even when designated as private, can be accessed in litigation, and otherwise distributed by friends of the user.

Social media users may be held responsible and subject to discipline for commentary that references the district, its staff, students, or operations in an inappropriate or illegal manner. In general, social media users should further be aware that they may incur liability arising from commentary deemed to be proprietary, copyrighted, defamatory, libelous, or obscene (as defined by law).

Social media users should take responsibility and monitor their own social media applications on a regular basis in order to review and approve any and all comments that may appear. Any inappropriate, offensive, obscene, or illegal comments or spam should be deleted or removed as soon as reasonably practical by the employee.

Employees should not permit students to comment on their personal social networking page or on their blog.

Prohibited Conduct

Employees are hereby advised that any and all district-related information published by the employee on their blog or social networking sites must comply with the district's Acceptable Use and Personal Conduct policies. Further, the employee must comply with confidentially obligations imposed by law, including HIPAA and FERPA. Employees must respect all copyright laws and must reference or cite all sources as required by law. Under no circumstances may the employee use district logos, mascots, or images on a personal social media account, profile, site, or blog without express written consent. The use of images or photographs of students on a personal blog or social networking webpage are absolutely prohibited.

Under no circumstances should employees discuss situations involving employee or student discipline on social media networks or sites. As a general guideline, employees should not post anything that they would not want to read in a newspaper or on a billboard.

Employees should not use the district's name to promote or endorse any product, cause, or political party or candidate.

Conduct in the Use of Social Media

Under no circumstances shall the use of social networking activities interfere with the employee's work obligations. Users may not use commercial social media during their work, school, and/or volunteer responsibilities unless approval has been granted by the Superintendent or designee, and only in circumstances where the social media has been opened for that person(s) and purpose only.

Employees should be aware that even privacy settings are not fool-proof. Search engines can turn up posts and pictures years after they have been published to the internet. It is recommended that employees keep their status as professionals and representatives of the district in mind at all times when communicating via social media.

Employees should use care in posting or publishing photos of themselves. Only pictures that they would be comfortable sharing with the parents of district students or their employer should be posted.

Employees should monitor pictures posted by their friends, utilize appropriate privacy settings, and monitor any tagging of their names to ensure that a search for the employee's name does not bring up inappropriate or unauthorized images of the employee.

Discipline Under This Policy

Violation of this policy by an employee will result in discipline as appropriate, up to and including termination, in accordance with all applicable district disciplinary policies and procedures.

Employees will be held responsible for the disclosure, whether purposeful or inadvertent, of confidential or proprietary information, information that violates the privacy rights of others.

Exceptions to this policy may be recognized in instances where employees' speech is made as a private citizen, on matters of purely public concern, where appropriate and where otherwise required by law.

Preservation and Compliance with Applicable Law

Nothing in this policy shall be interpreted in a manner that violates an employee's civil or other rights as set forth in state and federal law.

Book	Policy Manual
Section	800 Operations
Title	District Email
Code	816
Status	Active
Adopted	July 24, 2008
Last Revised	April 28, 2022

Purpose

It is the policy of the Hazleton Area School District (HASD) to: [1]

1. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications.

2. Prevent unauthorized access and other unlawful online activity.

3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors.

4. Comply with the Children's Internet Protection Act.

This policy describes guidelines of the Hazleton Area School District with regard to access to, retention of, and disclosure of electronic mail (email) messages sent or received with use of the HASD email system.

Authority

The Hazleton Area School District respects individual privacy; however, privacy does not extend to the employee's work-related conduct, the student's school related conduct, or to the use of district-provided equipment or supplies. Employees and students should be aware that the following guidelines might affect their privacy in the District's physical and virtual environment. Employees and students shall have no expectation of privacy while utilizing the district email, computers, networks, Internet access, and all other district systems. [1]

Personal Use

HASD provides employees and students with email accounts to assist in the process of education and learning. These email accounts must only be used in support of the educational objectives of the Hazleton Area School District. Each user is personally

responsible for their email account and operating it in accordance with this policy, the Acceptable Use policy, and any and all other applicable district policies. [1]

Email should not be considered a secure means of communication. Email should not be used for the transmission of sensitive or confidential information.

Inappropriate Use

The email system of the HASD may not be used in any way that may be seen as insulting, disruptive, offensive by other persons, or harmful to employee or student morale, or otherwise in violation of the district Acceptable Use policy or any and all other district policies. [1]

Prohibitive actions include, but are not limited to:

1. The use of HASD email for personal gain.
2. Sharing your email account password.
3. Infringing on the copyright or intellectual property of third parties.
4. The sending of chain letters or spam email.
5. The distribution of offensive messages or images.
6. Any illegal activity not specifically mentioned.

The email system may not be used to send offensive or pornographic content. Employees who transmit or store this material on HASD systems are subject to immediate termination through due process.

Users of the District's email system may not intentionally intercept, read, or alter another person's email. Additionally, users may not alter an email to fraudulently identify themselves, to conceal their true identity, to impersonate another user or the district, or maintain or establish anonymity in any other manner.

Appropriate School Use

Only an HASD email address should be used when communicating on behalf of HASD. The use of non-HASD email accounts for any HASD related functions is prohibited. Users are not permitted to use third party email systems (such as Yahoo, Gmail, or Hotmail) when using district devices, when using the district network, in communications between faculty and students, or in the capacity as an employees of HASD.

Confidentiality and Access

This electronic mail system has been installed by the HASD to facilitate educational communications. Although each user has an individual password to access this system, the system belongs to the HASD. The contents of email communications are vulnerable

to subpoena by the courts and discovery by third parties in litigation. Therefore, users should not assume that messages are confidential. Back-up copies of email shall be maintained and referenced by the district.

System administrators are authorized to take reasonable actions to implement and enforce district policy and ensure network security.

Email may be monitored to ensure the system functionality and accessed to perform regular system maintenance. Emails will not be examined without the prior authorization of the Hazleton Area School District Superintendent.

Delegation of Responsibility

The Hazleton Area School District Superintendent shall be the primary contact for the interpretation, enforcement, and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to the HASD solicitor for advice.

The Hazleton Area School District Superintendent authorizes system administrators to perform general inspection and monitoring to ensure the security and stability of the network and systems connected to it. This may include monitoring, inspection, and support activities such as, but is not limited to:

1. Assuring adequate quality of service for critical applications.
2. Detecting unauthorized use of the network.
3. Filtering content (as described above).
4. Preventing or investigating system problems or efficiencies.
5. Assessing security vulnerabilities of computers connected to the network.
6. Preventing or investigating improper or illegal activities.
7. Compiling usage statistics.

System administrators have the following responsibilities for systems and networks they administer:

1. Taking precautions against theft or damage.
2. Protecting the integrity of district networks, hardware, software, and privacy of personal, financial, and other confidential information stored on district systems and networks.
3. Following appropriate practices for security and disaster recovery.

4. Promulgating policies and procedures that govern services, access, and use of the systems they administer.

5. Reporting suspected legal violations, security threats or violations of district policy to appropriate district authorities.

6. Cooperating with administrators to find and correct problems caused by the use of systems under their control.

Guidelines

Suspension of Privileges and Consequences for Violation

System administrators may temporarily suspend access privileges if they believe it necessary to maintain the integrity of computer systems or networks. If legal violations, security threats, or violations of district policy are suspected, appropriate district authorities will be informed. Where appropriate, violations of this policy will be reported to appropriate legal authorities where the action in violation of the policy is believed to be in violation of criminal law. Further, where a user violates this policy in a manner in violation of the district's rights as protected by law, the district may pursue a suit against the user in the district's sole discretion.

Email Retention

All incoming, outgoing and internal emails for the Hazleton Area School District will be archived in accordance with the Federal Rules of Civil Procedure.

All emails arriving to HASD will first be filtered for spam. Emails determined to be spam will not be delivered to a user's inbox or archived. Any message delivered to or sent from a mailbox on the hasdk12.org domain will be archived according to this policy.

HASD will begin archiving all HASD email on October 1, 2010, at 12:01 a.m. Archived data will be retained for a period of two (2) calendar years from the date they are first archived. This will allow for messages to be indexed, stored and deleted once the retention date has been reached.

All email communication is subject to search and is the property of HASD. Deleting email from your inbox does not delete the email from the archive. Once an email has been sent and/or received in your inbox, the email will become part of the archive. There is nothing HASD can do to remove messages from the archive.

The archival solution also allows for email retrieval, search, and review by the request of administration or in the event of an investigation.

In the case of litigation, the administrative offices will notify the Technology Department, in writing, with the appropriate information necessary to place a litigation hold on select archived accounts or to suspend any archival data destruction until further notice. Once completed, the administrative offices will notify the Technology Department by writing to resume data destruction procedures according to this policy. [2]

Policy Interpretation

The Hazleton Area School District Superintendent shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

Legal
1. Pol. 815
2. Pol. 800
Federal Rules of Civil Procedure
Pol. 317
Pol. 814
Attachments:
816 Attachment I - Employee Acceptable Use Agreement Form
816 Attachment II - Non-District Employee AUP Form
816 Attachment III - Student Technology Acceptable Use Agreement

Book	Policy Manual
Section	800 Operations
Title	Copyright Material
Code	814
Status	Active
Adopted	August 18, 2011

Authority

The Board emphasizes that federal law makes it illegal for anyone to duplicate copyrighted materials without permission. The Board acknowledges that severe penalties are provided for unauthorized copying of audio, visual, software, online or printed materials unless the copying falls within the bounds of the fair use doctrine.[5]

Definition

Copyrighted materials include original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated.

The owner of the copyright is granted exclusive rights to do and to authorize any of the following:

1. Reproduce the copyrighted work.
2. Prepare derivative works based upon the copyrighted work.
3. Distribute copies of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending.
4. Perform the copyrighted work publicly.
5. Display the copyrighted work publicly.

Under the fair use doctrine, unauthorized reproduction of copyrighted materials is permissible for such purposes as criticism, comment, news reporting, teaching, scholarship or research. In order for the duplication or alteration of a product to fall within the bounds of fair use, four (4) standards must be met:

1. *Purpose and Character of the Use* – The use must be for such purposes as teaching or scholarship and must be nonprofit.

2. *Nature of the Copyrighted Work* – Staff may make single copies of: book chapters for use in research, instruction or preparation for teaching; articles from periodicals or newspapers; short stories, essays or poems; and charts, graphs, diagrams, drawings, cartoons or pictures from books, periodicals or newspapers.

3. *Amount and Substantiality of the Portion Used* – Copying the whole of a work cannot be considered fair use; copying a small portion may be considered fair use if appropriate guidelines are followed.

4. *Effect of the Use Upon the Potential Market for or Value of the Copyrighted Work* – If resulting economic loss to the copyright holder can be shown, making even a single copy of certain materials may be an infringement; and making multiple copies presents the danger of greater penalties.

Delegation of Responsibility

Staff may make copies of copyrighted school district materials that fall within the established administrative regulations. Where there is reason to believe the material to be copied does not fall within the administrative regulations, prior permission shall be obtained from the principal.

Each school principal shall establish practices and procedures to enforce this policy at the school level and shall address the issue of copyright at regularly scheduled faculty and staff meetings annually.

Staff members who fail to adhere to this policy may be held personally liable for copyright infringement.

Violations or questions of copyright should be directed to the principal or Superintendent or designee.

Staff members shall be responsible for instructing students in fair copyright practices and academic integrity, including guidance on citing resources appropriately.

Guidelines

Copyright notices shall be posted in all computer labs and on photo copy machines.

Computer software shall be licensed in accordance with Board policy and administrative regulations. All multiple user and site licenses must be kept on record at the district Media Center office. A copy must also be kept at the school licensed to use the software, in the custody of the building principal.[4]

All copyrighted materials designated for loan at the district Media Center must display a notice of copyright.

Videotapes/Video Discs/Audiovisual Delivery Devices

A library, archive, or media center may reproduce one (1) copy of a recording of a copyrighted work and distribute it in accordance with provisions of law.[6]

Recorded copies of copyrighted programs owned by a staff member **or** another person, or a copy of a rental program, are considered illegally made and may not be used for instructional purposes unless its use meets the fair use test.

Rental videocassettes, DVDs, video files and other optical media with the "home use only" warning label may not be used in a classroom, school assembly, or club unless specifically covered in the rental agreement.

Multimedia use of copyrighted material falls under the guidelines of the medium being used, such as computer, video, or audio.

Closed-circuit distribution of a copyrighted work to classrooms in a school or campus is legal, as long as the transmission is used for instructional activity and not entertainment.

Distance Learning

Distance learning is subject to copyright guidelines if copyrighted material is copied or recorded during a transmitted lesson.

The district shall limit the transmission of copyrighted materials to students enrolled in a particular course, to the extent technologically feasible.

Students shall be notified that materials used in connection with a course may be subject to copyright protection.

Technological measures shall be applied to ensure that copyrighted material is accessible to recipients only as long as class is in session.

The district shall not interfere with technological measures used by copyright owners to prevent unauthorized retention or dissemination.

Off-Air Recordings

Broadcast programs may be recorded off-air simultaneously with broadcast transmission, including simultaneous cable transmission, and retained by the district for a period not to exceed forty-five (45) consecutive calendar days after the date of recording. After this period of time, all recordings must be erased or destroyed immediately.

Off-air taping of broadcast programs is permitted by educational institutions for programs broadcast to the general public. Pay cable TV services and satellite broadcasts available at an extra charge are not allowed without permission from the copyright owner.

Program recordings may be used once by individual teachers in the course of relevant teaching activities, and repeated once only when instructional reinforcement is necessary, during the first ten (10) consecutive school days in the forty-five (45) calendar day retention period.

After the first ten (10) consecutive school days, off-air recordings may be used up to the end of the forty-five (45) calendar day retention period only for evaluation purposes by the teacher.

Off-air recordings may be made only at the request of and use by individual teachers and may not be regularly recorded in anticipation of requests. No broadcast program may be recorded off-air more than once at the request of the same teacher, regardless of the number of times the program may be broadcast.

Off-air recordings need not be used in their entirety; but they may not be altered from their original content and may not be physically or electronically combined or merged to constitute teaching anthologies or compilations.

All copies of off-air recordings must include the copyright notice on the broadcast program as recorded.

Computer Software

Copies of software, including those downloaded via modem, other than public domain software, cannot be made without the permission of the vendor or copyright owner.

Illegal copies of copyrighted programs may not be made or used on school equipment.

A computer program may be legally copied only for the following reasons:

1. It is created as an essential step in the use of the computer program, such as automatic copying into memory when a program is loaded.

2. It is created as a backup or archival copy only. All backup and archival copies must be destroyed in the event the original program is erased or removed from inventory.

Backup or archival copies may not be used simultaneously with the original program.

Copying a copyrighted program from a computer hard drive to a disc or server file for use as an additional copy is illegal.

Networking computer software is illegal if the legal multiple user or site licenses have not been acquired from the vendor or copyright owner. Networking is the use of a single program in a single computer that is connected to other computers, permitting the program to be used simultaneously in more than one (1) computer.

Reproduction of original computer software manuals is illegal, and copying must abide by the fair use guidelines.

The district will provide expenditures for software as a budgetary item. Priority will be given to software that supports and/or is critical to curriculum or operating needs. All other software will be purchased if reasonable need is established and/or financial resources allow such purchase.

Renting or lending original copies of software by individuals without the express permission of the copyright owner is illegal.

District staff must register all software, including software downloaded from the Internet, with the designated technology staff in accordance with Board policy.[4]

Legal
4. Pol. 815.3
5. 17 U.S.C. 101 et seq
6. 17 U.S.C. 108
17 U.S.C. 101 et seq
Pol. 000