FHS One-to-One Laptop Program Guidelines

Philosophy

Freedom Area High School's One-to-One initiative is designed to transform teaching, learning, and assessment at the secondary level. We believe that infused technology accomplishes the following goals:

- Increased academic rigor preparing students for post-secondary success.
- Increased student engagement in classrooms through meaningful integration of technology.
- Facilitating our adopted Instructional Model with a differentiated approach.
- "Levels the playing field" allowing equal access to technology for **all** students.

Laptop Use Guidelines

The laptops are the property of the Freedom Area School District. They will be assigned to high school students enrolled at the high school in courses that require this use once the parent/guardian has signed off on the responsibility agreement (Addendum A). Laptops must be returned to the Freedom Area School District at the conclusion of each school year, or when a student unrolls/moves. The laptop must be returned in original working condition. The laptops are only educational tools and are to be used only in that capacity. Students using laptops are bound by the Freedom Area School District's Acceptable Use Policy (Addendum B). The policy is available through the high school web site (www.freedom.k12.pa.us) as well. The use of the laptop is a privilege that can be revoked upon violation of this Policy. Inappropriate use or neglect of a laptop, the internet, the school network or any installed software will result in disciplinary action (Addendum C).

Internet and Software Guidelines

The FASD Acceptable Use Policy must be followed at all times. **Students should have no expectation of privacy related to laptop use and can expect teachers, technical support staff and administrators to conduct spot checks of their Internet history and usage data.** Logs and other records of usage will be checked as well. Students may not install or run software that has not been approved by administration.

General Rules

- Students will carry their laptops throughout the school day and are responsible for the laptop at all times. For the protection of the laptop, ***it is required that they be stored and carried in a protective bag when not in use.***
- Students are not authorized to use other student's laptops. Sharing machines is prohibited.
- Students may not use the laptops on buses.
- Students may not use laptops in the cafeteria during lunch.
- If a student is unable to carry and supervise his/her laptop, it is to be locked in the individual student's assigned locker. It is the student's responsibility to provide a lock.
- Students must keep their passwords confidential.
- Students are responsible for regularly backing up school documents on their Google docs account or external storage device. Failure to back up documents does not constitute an excuse for not turning work in on time. If a hardware failure occurs student work may be lost.

- Obscene language and/or inappropriate screensavers, backdrops and/or pictures are strictly prohibited.
- Illegal use or transfer of copyrighted materials is prohibited.

General Operating Guidelines

- Do not mark the laptop in any way; no stickers or other decorations are permitted.
- Do not remove school identification or name tags from the laptop.
- Do not share lockers when storing laptops.
- Food and drink is not to be used near the laptop.
- Use the laptop on a flat, stable surface.
- Students are responsible for reporting any technical issues or damage affecting the performance of the laptop to a member of the technical staff or administration. This needs to occur in a timely manner to ensure loaner laptop availability.

Charging and Cleaning Guidelines

- Enter school each day with a fully charged laptop. Students will have the opportunity throughout the day to charge their laptop in specified areas.
- Failure to charge the laptop is equivalent to not being prepared for class.
- Do **NOT** use water or other cleaning solutions on the laptop. Student should visit the "Technology Help Center" for proper cleaning of their computer.

Technology Maintenance Fee

Each student in the One-to-One program will be required to pay an annual technology maintenance fee of $50.00. This fee will be used to cover maintenance, repair and software upgrades. **Intentional laptop damage, as determined by district staff, will not be covered.** The entire cost to repair or replace intentionally damaged machines falls on the student/parent. Multiple repair claims by any one student will be reviewed and appropriate action taken. Action may include a ban on taking the computer from the building.

Repair Policy

The $50.00 annual maintenance fee will cover all repairs to the laptop as long as there is no evidence of vandalism or misuse. In case of loss, theft, misuse or vandalism, the following approximate costs will be incurred by the parent and paid to Freedom Area High School.

A. Keyboard Breakage:	$50.00 - $75.00
B. Screen Breakage:	$150.00 - $200.00
C. Plastic Case Replacement:	$30.00 - $40.00
D. Charger Replacement:	$30.00 - $60.00
E. Battery Replacement:	$90.00 - $100.00
F. Hard Drive:	$50.00 - $75.00
G. Loss/Theft:	According to Scale (Addendum D)

FASD Student-Parental One to One Responsibility Agreement

_____ and his/her parent/guardian have fulfilled all of the requirements to receive a laptop:

1. Parent & Student attended Laptop Orientation Session. (Freshman/New Students only)
2. Agrees to Freedom Area High School One-to-One Laptop Guidelines.
    a. All repairs from normal wear and tear are covered by the school. **In case of accidental damage, loss, theft, repeated misuse or vandalism, all associated repair costs will be incurred by parent and paid to the Freedom Area High School**.
3. I understand that by signing below, I have read and agreed to the Freedom Area High School:
    a. A. Acceptable Use of Technology Policy 815
    b. Freedom Area High School One-to-One Laptop Guidelines and will be liable for associated costs.

Signature of Student _____

Signature of Parent/Guardian _____

Date _____

Payment received - $50.00 Check#_____ Cash _____

FREEDOM AREA SCHOOL DISTRICT

POLICY 815

ACCEPTABLE USE OF TECHNOLOGY SIGNATURE PAGE
FOR PARENT/GUARDIAN/STUDENT

I understand and will abide by the terms and conditions of Policy #815, Acceptable Use of Technology, of the Freedom Area School District. I further understand that any violation of the regulations as outlined in the preceding pages is unethical and may constitute a criminal offense. Should I commit and violations, my access privileges may be revoked, and school disciplinary and/or appropriate legal action may be taken.

Student Signature _____ Grade _____ Date_____

As the parent/guardian of this student, I have read the terms and conditions of Policy #815, Acceptable Use of Technology, of the Freedom Area School District. I understand that this access is for educational purposes; however, I also recognize it is impossible to restrict access to all controversial materials and I will not hold the Freedom Area School District responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child uses the Internet, Local Area Networks, etc., outside of school sponsored activities. I herby give permission for my child to use the World Wide Web and certify that the information contained on this form is correct.

Parent/Guardian _____
(Please print name)

Signature _____Date_____

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Number	815
Status	Active
Adopted	November 14, 1996
Last Revised	October 14, 2010

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 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:[25]

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.[26]

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:[27]

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:[27]

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 obscene, child pornography or harmful to minors.[3]

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.

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, 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 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][7][8]

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.[9][10][11][12][13][14][15]

5. Bullying.[16]

6. Terroristic.[17]

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. 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. [18][2][3]

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.[18]

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.[19][2]

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 web site, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[18]

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 tracking systems to track and recover lost or stolen equipment.

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][22]

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 web sites and in chat rooms.

2. Cyberbullying awareness and response.[21][16]

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.

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, e-mail, social networking web sites, etc.

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

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.[22]

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 by minors, 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 nonschool-related work.

4. Product advertisement or political lobbying.

5. Bullying.[21][16]

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.[23]
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. [24]
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.

Security

System security is protected through the use of passwords. 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.[25][24]

District Web Site

The district may establish and maintain a web site 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 web site shall comply with this and other applicable district policies.

Users shall not copy or download information from the district web site 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.[18]

Illegal use of the network; intentional deletion or damage to files or data belonging to others; 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][7][8]

Legal

2. 20 U.S.C. 6777

3. 47 U.S.C. 254

4. Pol. 218

5. Pol. 233

6. Pol. 317

7. Pol. 417

8. Pol. 517

9. Pol. 103

10. Pol. 103.1

11. Pol. 104

12. Pol. 248

13. Pol. 348

14. Pol. 448

15. Pol. 548

16. Pol. 249

17. Pol. 218.2

18. 24 P.S. 4604

19. 24 P.S. 4610

21. 24 P.S. 1303.1-A

22. 47 CFR 54.520

23. Pol. 237

24. Pol. 814

25. 17 U.S.C. 101 et seq

24 P.S. 4601 et seq

25. 18 U.S.C. 2256

26. 18 Pa. C.S.A. 6312

27. 18 Pa. C.S.A. 5903

Pol. 220

815-Attach.doc (27 KB)

Technology Violations and Disciplinary Actions

Addendum C

	Level I - Nuisance Violations: Including but not limited to, downloading games, music, software, file sharing including limewire, bit torrent or other similar service.	**Level II - Ethical Violations: Including but not limited to , downloads of pornographic images or movies, copyrighted material (music, TV shows, movies).**	**Level III - Network Security Violations: Including but not limited to, password theft, network attack, hacking of network or internet, identity theft, and inappropriate use of bandwidth.**
First Offense	Teacher Takes Laptop	Teacher Takes Laptop	Teacher Takes Laptop
	Machine Reimaged	Machine Reimaged	Machine Reimaged
	Parent is Notified	Meeting with parent	Meeting with Parent
			Student Loses Laptop for 10 Days
Second Offense	Same as First Offense	Student Loses Laptop for 10 Days	3 Day Suspension Loss of Laptop for 20 Days Network Privleges Revoked - Wireless Card Removed
	Meeting with Parent Before Laptop is Returned to Student		
Third Offense	Student Loses Laptop for 5 Days	3 Day Suspension and Loss of Laptop Use for 10 Days	
Fourth Offense	3 Day Suspension and Loss of Laptop Use for 10 Days	Network Privileges Revoked - Wireless Card Removed	

Addendum D

Sliding Scale for Loss or Theft of a Laptop

Age of the machine at the time of loss or theft	Cost to student/family
0 - 1 Years	100% of purchase price
1 - 2 Years	90% of purchase price
2 - 3 Years	80% of purchase price
3 - 4 Years	70% ofpurchase price
4 - 5 Years	60% of purchase price
5 - 6 Years	50% of purchase price

The cost will apply to all machines that are reported lost or stolen