Eastern Lancaster County School District
Empowering Learners as Global Thinkers and Producers

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Code	815
Status	Active
Adopted	May 15, 2023

Purpose

The Board supports use of District technology 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, contractors, and other authorized individuals with access to the District's computers, mobile devices, systems, and network, which includes Internet access, whether wired or wireless, or by any other means.

For instructional purposes, the use of District technology 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

District Technology - all technology owned, operated, and/or licensed by the District, including networks, audio/visual equipment, sound systems, software, printers/scanners, internet access, mobile devices, computers, computer peripherals, information systems, data, social media accounts, data storage, Internet of Things (IOT) devices, and account credentials used to access such resources.

User - anyone who utilizes or attempts to utilize District technology while on or off District property. The term includes, but is not limited to, students, staff, contractors, parents and/or guardians, and any visitor to the District who may use District technology.

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:[1]

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.[2]

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:[3][4]

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:[5]

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:[5]

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.[4]

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 District technology 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 District technology.

The Board declares that the use of District technology is a privilege, not a right. The District's technology 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 or other District technology including personal files The District reserves the right to monitor, track, and log technology 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 any District technology.[6][7][8]

District technology must be used only by the people to whom it has been issued. The person to whom the technology resource was issued is ultimately responsible for any actions performed on the device.

Users must always protect District technology, keeping it physically and logically secured and under the control of the user.

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:[4]

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.[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. 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.[3][4][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]

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 technology resources are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[3][4][16]

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 digital citizenship including:[4]

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

2. Cyberbullying awareness and response.[12][17]

Guidelines

Use of Personal Electronic Devices

The use of personal electronic devices on the District network is permitted only on the designated "Guest" network. When a user connects a personal electronic device to a District network or to District technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a District-owned device were being utilized. Users who connect a personal electronic device to a District network explicitly waive any expectation of privacy in the content exchanged over the District technology resources.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Users are prohibited from using any type of District provided account that does not belong to them and are prohibited from using platforms to impersonate others. All users shall respect the privacy of other users on District systems and networks.

Safety

It is the District’s goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any 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. Users shall not reveal personal information to other users on the network/internet, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[4][16]

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 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 digital citizenship , 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/Cyberbullying.[12][17]
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.[18]
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.[19]
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 District technology.
18. Accessing District technology 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 and multi-factor authentication where possible. 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.[19][20]

Consequences for Inappropriate Use

Users of District technology shall be responsible for damages to District technology resulting from deliberate or willful acts.[14]

Illegal use of District technology ; 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.[6][7][8]

Limitation of Liability

The District makes no warranties of any kind, whether express or implied, for the service it is providing through its various District technology, therefore it assumes no liability for direct and/or indirect damages arising from the user's use of such District technology, information systems, and/or technology services. Use of District technology by the user is at the user's own risk.

Users are solely responsible for the content they disseminate. Eastern Lancaster County School District is not responsible for any third-party claim, demand, or damage arising out of use of Eastern Lancaster County School District technology, information systems, and/or technology services.

Legal

1. 18 U.S.C. 2256
2. 18 Pa. C.S.A. 6312
3. 20 U.S.C. 7131

4. 47 U.S.C. 254

5. 18 Pa. C.S.A. 5903

6. Pol. 218

7. Pol. 233

8. Pol. 317

9. Pol. 103

10. Pol. 103.1

11. Pol. 104

12. Pol. 249

13. Pol. 218.2

14. 24 P.S. 4604

15. 24 P.S. 4610

16. 47 CFR 54.520

17. 24 P.S. 1303.1-A

18. Pol. 237

19. Pol. 814

20. 17 U.S.C. 101 et seq

18 Pa. C.S.A. 2709

24 P.S. 4601 et seq

Pol. 220