Book: Policy Manual
Section: 800 Operations
Title: Use of the Internet and the District's Network
Number: 815
Status: Active
Legal:
1. Pol. 218
2. Pol. 233
3. Pol. 317
4. Pol. 417
5. Pol. 517
7. 20 U.S.C. 6777
8. 47 U.S.C. 254
9. 24 P.S. 4604
10. 24 P.S. 1303.1-A
11. Pol. 252
12. Pol. 248
14. 47 CFR 54.520
15. Pol. 814
16. 18 U.S.C. 2256
17. 18 Pa. C.S.A. 6312
18. 18 Pa. C.S.A. 5903
24 P.S. 4601 et seq
17 U.S.C. 101 et seq
Adopted: May 23, 2017
Last Revised: May 9, 2017
**Purpose**

The District is committed to ensuring internet safety to the greatest extent possible. This Policy governs the appropriate use of the District’s network, District-owned technology and the internet, as set forth, below. The provisions of this policy apply to all use of the District’s network, both on and off campus as well as student and employee access to/use of the internet during school hours, on school grounds and during school-sponsored activities.

**Authority**

Access to the School district’s network is a privilege, not a right. The school district reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The school district will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the District’s network. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604.

The school district reserves the right to:

1. Discontinue network availability and/or access at any time for any or all users for any reason;
2. Determine which network services and/or District technology will be provided through school district resources;
3. Determine the types of files that may be stored on school district file servers and computers;
4. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the District’s network and electronic communications systems and/or on District technology, including e-mail, text messages, and other electronic communications; fileserver space, processor, and system utilization, and all applications provided through the District’s network and electronic communications systems and/or on District technology, including e-mail, text messages, and other electronic communications;
5. Remove from the network, District servers or District-owned devices excess e-mail and other electronic communications or files for any reason; and
6. Revoke user privileges, remove user accounts, or refer to legal authorities, and or school district authorities when violation of this and any other applicable school district policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, and destruction of School district resources and equipment.

**Definitions**

**Child Pornography** - Under federal law, this term means 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. 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.

Under Pennsylvania law, the term means 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.

For the purposes of this Policy, Child Pornography includes material/content that meets either the Pennsylvania or the federal standard or both

**District-Owned Devices / District-Owned Technology** – Definition shall be consistent with Board Policy 815.2

**Harmful to Minors** - Under federal law, this term means any picture, image, graphic image file or other visual depictions that:

1. Is taken as a whole, with respect to minors, appeals to the 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 content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals.
3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors.

Under Pennsylvania law, this term means any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

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

For the purposes of this Policy, “harmful to minors” includes material/content that meets either the Pennsylvania or the federal standard or both.

Incidental Personal Use – This term refers to use of the internet by District that does not interfere with the employee’s job duties and performance, with system operations, or with other system users. Incidental personal use must comply with this policy, accompanying administrative procedures, and all other applicable school district policies, regulations, procedures and rules, as well as ISP terms, local, state and federal laws, and must not damage the school district’s systems.

Minor – This term, for purposes of compliance with the Children’s Internet Protection Act (“CIPA”), an individual who has not yet attained the age of seventeen (17). For other purposes, “minor” shall mean the age of minority as defined in the relevant law.

The term “network,” for the purposes of this Policy, includes the District’s server(s) and any and all access to the information stored thereon, whether retrieved Network – through a wired device or wireless access, including the use and/or access to the internet or other servers or networks through the District’s server. The term also expressly includes any system linking two (2) or more District-owned electronic devices.

Obscene - under federal law, analysis of the material meets the following elements:

1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.
2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene.
3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

Under Pennsylvania law, analysis of the material meets the following elements:

1. The average person, applying contemporary community standards, would find that the material, 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.
3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.

For the purposes of this Policy, “obscene” includes material/content that meets either the Pennsylvania or the federal standard or both. For the purposes of this Policy, “obscene” shall also include any and all gratuitous nudity or partial nudity without social or artistic value or nude/partially nude images that are being accessed for prurient purposes, regardless of the image’s intrinsic social or artistic value. This definition shall expressly include all forms of sexting and the sending, viewing or possession of nude or partially nude photographs via cell phone, email, internet, social media, or other electronic form.

Sexual Act and Sexual Contact – This term shall be interpreted consistent with 18 U.S.C. Sec. 2246, and at 18 Pa. C.S.A. Sec. 5903.

Social Media – The term “social media,” for the purposes of this Policy, includes all web-based services that allow individuals to (1) construct a public, semi-public or private profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections made by others within the system. Such sites include Facebook and MySpace. The term shall also expressly include all other interactive websites, such as blog sites and microblogs (such as Twitter), virtual worlds (such as World of Warcraft, Second Life), video/audio/photo sharing sites (such as Instagram, Pinterest, YouTube, Flickr, photo upload sites, etc.), instant messaging, podcasts, chatrooms and other interactive online forums. This term shall also expressly include all non-District email accounts and sites. This term expressly excludes collaborative websites that are contained within the District’s web domain (www.eastonsd.org) or District-sponsored collaboration sites for which the building or District administration has approved and has provided assurance, in writing, that the site does not permit collaboration by members of the public outside of the school, meets the safety and quality standards and requirements set forth in this Policy.
Technology Protection Measure(s) – This includes, but is not limited to, the use of a specific technology or specific technologies that block(s) or filter(s) internet access to visual depictions that are obscene, child pornography or harmful to minors. 47 U.S.C. § 254(h)(7)(I); 24 P.S. § 4606.

Visual Depictions – This term includes undeveloped film and videotape, and data stored on a computer disk or by electronic means which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words. 18 U.S.C. § 1460 (b); 18 Pa.C.S.A. § 2256.

Delegation of Responsibilities
The Superintendent is granted the authority to create administrative procedures to accompany this policy. The administrative procedures must include, among other sections: Prohibitions (General Prohibitions, Access and Security Prohibitions, and Operational Prohibitions), Content Guidelines, Due Process, Search and Seizure, and Selection of Material. This policy must be incorporated into the administrative procedure. The Superintendent is also granted the authority to create an administrative procedure that specifically addresses teacher-student communication when social networking tools are used. It shall be the responsibility of each building administrator to ensure that this Policy is followed appropriately in his/her building and to determine what is an acceptable use of the internet under this Policy and any accompanying administrative procedures. It is the responsibility of the Supervisor of Information Systems to ensure that the network is properly maintained in accordance with the guidelines set forth in this Policy.

Requirements

1. Acknowledgment and Consent
A copy of this policy and EASD Acceptable Use Form will be provided to all users, who must be presented with the school district’s EASD Acceptable Use Form to sign. Users must be capable and able to use the school district’s systems and software relevant to the employee’s responsibilities.

2. Internet/Network Use Restricted to Educational Purposes
Use of the District’s network and the internet is limited exclusively to use for educational purposes. Personal and/or recreational use of the internet shall not be permitted on the District’s network.

3. Non-Network Access Prohibited
All access to the internet by students while on school grounds or at school-sponsored functions/trips must be through the District’s network. Access to the internet during school hours via 3G/4G-capable devices or other non-District connections is prohibited. In circumstances, which may be related to a student's disability, permission to utilize non-district connection must be requested and granted through the Supervisor of Information Technology.

4. Internet Access / Restrictions on District Network
The District provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

The District may maintain a usage log and may monitor the online activities of minors using the District’s network.

Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it should not be, the user should follow protocol to alert an IT staff member or submit a work order. If a site is accessible that contains content that is permissible under this or another Board Policy, the user is required to immediately report it to the building principal.

Because of the nature of the filter and blocking technology, as well as the technology that allows the internet to operate, the District cannot ensure that all access to explicit, inappropriate or unlawful materials will be completely blocked. However, intentionally accessing such resources is inappropriate and will result in disciplinary action and/or denial of privileges.

5. Student Training
The District shall provide, at least once per school year, training to students regarding safety and the internet. This training shall include information about this Policy as well as additional information regarding appropriate online behavior, including proper interactions with other individuals on social networking sites and in chat rooms. The training shall also include information regarding cyber-bullying and appropriate responses to cyber-bullying.

6. District Email Accounts
The District provides users with email accounts for the purpose of school-related communication. Use of District email accounts for personal, non-school-related purposes is prohibited. The District reserves the right to revoke permission to use a District email account at any time for any reason.

Users are expected to utilize email accounts in an appropriate manner and in a manner that is mindful of the personal and network security risks. Students may not send personal information to unknown individuals or individuals that they have met online. Users should not attempt to open files or follow links from unknown or untrusted origins. Users should use appropriate language. Students are prohibited from communicating via email in a manner that violates the Code of Conduct, District policy or the rules/requirements of an individual teacher.

Email usage will be monitored and archived. Users are reminded that they have no expectation of privacy with regards to emails created/received on the District’s system. For safety reasons, the District may, at its discretion, conduct searches of District email accounts. The District has sole discretion to access, and maintain emails sent and/or received from a District account as it deems necessary/appropriate.

7. Student Use of Social Media Prohibited
Students are prohibited from using social media, as defined in this Policy, on the District’s network, during school hours and/or during school-sponsored activities unless such use is for a school project formally approved by the District that meets the requirements set forth in Board Policy 815.4 –

8. Security
Definition shall be consistent with Board Policy 815.2

9. Unauthorized Access
Unauthorized access would be considered hacking and logging into the network using another individual’s username and password. This act is strictly prohibited and will result in discipline and denial of privileges. Such unauthorized access may also result in a referral to law enforcement and potential criminal charges.

10. Personal Student Information
Users are prohibited from publishing on the internet or otherwise disseminating the personally identifiable information of students. Students who publish to the internet personally identifiable information about other students on the school’s network, during the school day, on school grounds or during school-sponsored activities may be subject to discipline and/or loss of privileges. District employees are required to comply with the Family Rights and Privacy Act (FERPA).

11. Downloads
Users are not permitted to download or attempt to download or run .exe programs over the school network or onto school resources without express permission from IT staff. Students are not permitted to download any file types, including images, photos, video or audio files, without permission from a teacher or administrator. For the security of the District’s network, users should download such files only from reputable sites and only for educational purposes.

12. Copyright
Federal and state copyright laws govern and restrict the permissible use of all material accessed on the District’s network and the internet.

13. Personal Safety
Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet allows potential perpetrators to interact anonymously with students, which bears associated risks. Users should carefully safeguard the personal information of themselves and others. Users should never agree to meet in real life, without parental permission, someone they initially met online.

Any student who receives threatening or unwelcome communication should report such communication immediately to a teacher or administrator. Employees should report such communications to their immediate supervisors or, if the communication is from such supervisor, directly to the building principal or District-level administrator. Students who receive threatening or unwelcome communication while at home or off-campus are encouraged to immediately report it to their parents or other adult. Harassing,
threatening or bullying communications made by District staff or students to other staff or students should be reported to District administration regardless of whether such communication was received during school hours, on school grounds or at school functions.

14. District Monitoring of Internet and Network Usage and Activity
The District reserves the right to monitor and log User activity on the District’s network, at its discretion. Users shall have no expectation of privacy for activity on the District’s network or while using a District-owned device. User network passwords prevent unauthorized individuals from accessing the District’s network without permission, however, such passwords are not required for authorized IT administrators and other District administrators to access an individual account. The Superintendent shall designate an individual or individuals who shall maintain this responsibility.

15. Cyber-bullying Definition shall be consistent with Board Policy 252

16. Prohibited Content
Users may not access materials that are obscene, contain child pornography or are harmful to minors. The building administration shall have the responsibility of determining whether content falls within these categories. Users are encouraged to use common sense and good judgment when accessing materials online. Employees who wish to access online content for educational purposes but are not sure whether such content falls within the above definitions of “obscene,” “child pornography” or “harmful to minors” are required to consult with the building principal.

The dissemination of explicit sexual materials to minors is unlawful and will be subject to discipline and possible criminal sanctions. This includes, but is not limited to, obscene materials, as set forth in 18 Pa. C.S.A. 6312.

17. Incidental Personal Use by Employees
Employees may engage in incidental personal use as a privilege, as defined in the “Definitions” section, above. Such use must be limited to occasional use only and must comply fully with the terms of this Policy and any accompanying administrative procedures. The District reserves the right to prohibit incidental personal use by all or specific employees for any reason, including where there is a history of misuse, where such use becomes a burden for the District’s technology or where enforcement of the incidental personal use requirements become too cumbersome. Where incidental personal use is prohibited by a specific employee or group of employees, the District must provide notification to such employee(s) of the prohibition of such use.

18. Expectation of Privacy
Students and staff are reminded that they have no expectation of privacy when using District-owned technology, its email system or its network.

19. Storage of Personal/Private Data on District Network
Users are not authorized to maintain personal and/or private data not related to the school or school business, including personal documents, emails, etc., on the District’s network. Personal data should not be maintained on District servers, and the District shall not be responsible for ensuring or safeguarding the security and/or confidentiality of such data. The District shall not be responsible for the loss of any personal or private data stored on the District’s network.

20. Limitation of Liability
The District makes no warranties of any kind, either expressed or implied, that the functions or services provided by or through the District’s computer network systems will be error-free or without defect. The District will not be responsible for damage or harm to persons, files, data, or hardware due to use of the District’s network.

While the District employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

The District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

The District will not be responsible for the loss of any data or information stored on the District’s network or on a District server, including emails and/or documents.

21. Policy Violations
The District reserves the right to hold students/employees responsible for damage that occurs.

22. Data Breach
In the event of a data breach of the District’s systems, the District shall comply with all applicable state and federal laws, including those requiring notice to those whose data may have been breached. The Superintendent or designee shall be responsible for ensuring compliance with the necessary laws.