Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Technology Resources
Code	815
Status	Active
Adopted	October 26, 2016
Last Revised	June 23, 2021

Purpose

The Intermediate Unit provides students, staff and other authorized individuals with access to the Intermediate Unit's computers, iPads, Cellular Phones, network, and technology resources, which includes Internet access, whether wired or wireless, or by any other means.

The Intermediate Unit's goal in providing this service to students, staff and other authorized individuals is to promote educational excellence in the tri-county area by facilitating resource sharing, innovation, and communication. With access to the Internet and technology resources comes the availability of material that may not be considered of educational value in the context of the school setting. Despite the availability of filters and blocking software, students, staff and other users may nevertheless gain access to electronic information that may not be reliable or appropriate. Users may also receive unsolicited communications. In such cases, general school rules and Intermediate Unit policies for behavior and communications shall apply.

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:[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.

Minor - for purposes of compliance with the federal Children's Internet Protection Act (fedCIPA), 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.

Obscene - any material or performance, if:

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.

Sexting - refers to taking, possessing, viewing, sharing, or sending pictures, graphic images, text messages, emails, or other material of a sexually explicit or suggestive nature on an electronic device.

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]

User - means anyone who utilizes or attempts to utilize Intermediate Unit technology resources while on or off Intermediate Unit property. The term includes, but is not limited to, students, faculty, staff members, parents/guardians, and any visitors, both adults and minors, to the Intermediate Unit that may use Intermediate Unit technology.

Vandalism - is defined as any malicious attempt to harm or destroy data or equipment of the Intermediate Unit, another user, Internet, or other networks: This includes but is not limited to uploading or creating computer viruses. Vandalism may result in disciplinary action, including loss of employment, restitution, and referral to law enforcement.

Visual Depictions - undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.

Authority

The availability of access to electronic information does not imply endorsement by the Intermediate Unit of the content, nor does the Intermediate Unit guarantee the accuracy of information received. The Intermediate Unit 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 Intermediate Unit shall not be responsible for any unauthorized charges or fees resulting from access to the Internet and technology resources.

The Board declares that computer and network use is a privilege, not a right. The Intermediate Unit's computer, iPads, Cellular Phones, network, and technology resources are the property of the Intermediate Unit. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the Intermediate Unit's Internet, computers, iPads, Cellular Phones, or technology resources, including personal files or any use of the Intermediate Unit's Internet, computers, iPads, Cellular Phones or technology resources. The Intermediate Unit reserves the right to monitor, track, and log network access and use; monitor file server space and cloud-based space utilization by users; utilize remote tracking to locate and recover lost or missing devices; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The Intermediate Unit 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 Intermediate Unit's Internet, computers, iPads, Cellular Phones and technology resources.[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 Executive Director 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 Intermediate Unit 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 Intermediate Unit operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers, iPads, and mobile devices used and accessible to adults and students. The technology protection measure shall be enforced during use of computers, iPads, and mobile devices with Internet access.[3][4][14]

Upon request by students or staff, the Executive Director 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]

Upon written request by students or staff, the Director of Innovative Technology Solutions or designee 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 Executive Director or designee for expedited review.[3][15]

Delegation of Responsibility

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

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

Users of Intermediate Unit networks or Intermediate Unit 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 Intermediate Unit 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.

The Executive Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the Intermediate Unit's computers, iPads, and mobile devices 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.

Guidelines

Safety

It is the Intermediate Unit'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, including email, social networking websites, mobile messengers, 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 email, social networking websites, mobile messengers, 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.

Staff Responsibility

Students shall:

1. Use the Internet and technology resources for educational purposes.
2. Keep private information private; student passwords and identity shall not be shared.
3. Treat others with respect, both online and offline.
4. Report anyone who tries to use technology to hurt or harass the student to a teacher or other adult.
5. Strive to be a digital citizen.

6. Encourage others to be good digital citizens.
7. Respect the work of others and not purposely copy, damage, or delete their work.
8. Engage in appropriate conversation in all interactions with others.
9. Ask for permission before connecting personal devices to the Intermediate Unit network.
10. Follow all Board policies and administrative regulations regarding technology.
11. Care for Intermediate Unit-owned equipment.

Students shall refrain from:

1. Accessing inappropriate material on the Internet, including but not limited to hate mail, discriminatory remarks, and/or offensive or inflammatory communication.
2. Using the Internet, technology resources, or communication services owned or leased by the Intermediate Unit for sending, receiving, reviewing or downloading written, audio, or visual depictions of pornography, obscenity, child pornography, or other materials that may be harmful to minors.[17]
3. Engaging in unauthorized access of computers, including "hacking."
4. Engaging in unlawful activities.
5. Revealing any personal identification such as home address, phone number(s), and password(s).
6. Revealing personal information of others.
7. Using the Internet and/or technology resources for commercial or for-profit purposes, product advertisement, political lobbying, or illegal activity.
8. Using the Internet and technology resources in a way that disrupts the work of others.
9. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting/impersonating other users on the Internet.

Internet communications are not guaranteed to be private, and individuals who operate the system do have access to electronic data. Communications relating to or in support of illegal activities may be reported to the authorities. Staff assisting students in creating student email addresses must use nondescriptive identifiers (such as numbers instead of names).

The illegal installation and/or utilization of copyrighted/unauthorized/unvetted games, programs, files or other electronic media on the Intermediate Unit's technology resources is prohibited.

The Intermediate Unit retains ownership and rights of access to all Internet and technology resources under the control of the Intermediate Unit.

The technology and network belong to the Intermediate Unit, and using them is a privilege, not a right.

Digital Citizenship

Digital citizenship is an important aspect of using the Internet and technology resources The Intermediate Unit encourages and strives to model digital citizenship. As part of the digital citizenship efforts, the Intermediate Unit will provide educational resources to staff to be used in educating students on network etiquette and appropriate online behavior including interacting with other individuals on social network websites and in chat rooms. Cyberbullying awareness and response will also be addressed. The Intermediate Unit will collaborate with participating entities to ensure students receive training from either their sending district or the Intermediate Unit.

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 Intermediate Unit 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

Intermediate Unit Website

The Intermediate Unit shall establish and maintain a website and shall develop and modify its web pages to present information about the Intermediate Unit under the direction of the Executive

Director or designee. All users publishing content on the Intermediate Unit website shall comply with this and other applicable Board policies.

Users shall not copy or download information from the Intermediate Unit website and disseminate such information on unauthorized web pages without authorization from the building administrator or program supervisor.

Consequences for Inappropriate Use

Users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[14]

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.

Violations of this policy or inappropriate use of the Internet, Intermediate Unit network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.[6][7][8]

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. Pol. 237

17 U.S.C. 101 et seq
18 Pa. C.S.A. 2709
24 P.S. 1303.1-A
24 P.S. 4601 et seq
Pol. 220
Pol. 814

AUP - employee.docx (41 KB) AUP - Student.docx (42 KB)