Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Code	815
Status	First Reading

Purpose

The Board supports use of the computers, Internet and other network resources in the Intermediate Unit'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 Intermediate Unit provides students, staff and other authorized individuals with access to the Intermediate Unit'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 Intermediate Unit 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:[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]

VPN - virtual private network extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Entity - any business unit, department, group, or third party, internal or external to Delaware County Intermediate Unit, responsible for maintaining Delaware County Intermediate Unit assets.

Risk - those factors that could affect confidentiality, availability, and integrity of Delaware County Intermediate Unit's key information assets and systems. Information Management & Technology staff is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

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 or other network resources.

The Board declares that computer and network use is a privilege, not a right. The Intermediate Unit’s computer and network 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 or network resources, including personal files or any use of the Intermediate Unit’s Internet, computers or network resources. The Intermediate Unit reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by users; deny access to prevent unauthorized, inappropriate or illegal activity; 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 and/or authorities in

any investigation concerning or related to the misuse of the Intermediate Unit's Internet, computers and network 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 and the Director of Information Technology, and/or designee.

In addition to those stated in law and defined in this policy, The Board establishes the following types of materials to be 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, 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 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 Executive Director or designee may expedite a review and may authorize the adjustment 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 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.

Student (minor) 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 Intermediate Unit and on the Internet.

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

The Executive Director or members of Executive Council shall be responsible for recommending technology and developing procedures used to determine whether the Intermediate Unit'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:[3][4][15]

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 Intermediate Unit should develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[4]

1. Interaction with other individuals on social networking websites and in chat rooms.
2. Cyberbullying awareness and response.[12][16]

The Executive Director or designee should develop other administrative regulations as necessary to the requirements of the policy.

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 Intermediate Unit’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:[4][15]

1. Control of access 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 Board policy and administrative directives, accepted rule 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][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.[17]
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, including use of another user's email address, user account or password.
14. Fraudulent copying, communications, or modification of materials in violation of copyright laws. [18]
15. Loading or using of unauthorized games, programs, files, unlicensed software 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, Intermediate Unit 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 to infiltrate or interfere with a computer system and/or damage the data, files, operations, software or hardware components of a computer or system, engaging in hacking in any form.
22. Use to misrepresent or assume the identity of other users on the network.
23. Posting anonymous messages.
24. Any attempt to circumvent or disable the filter or any security measure.

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 should not reveal their passwords to another individual.

2. Users are not to use a computer or software 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.

Remote Access

It is the responsibility of Delaware County Intermediate Unit employees, contractors, vendors and agents with remote access privileges to Delaware County Intermediate Unit's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Delaware County Intermediate Unit.

1. Remote access to DCIU network and data resources can only be implemented via DCIU provided VPN connection.

2. Remote access to DCIU network can only be implemented from DCIU provided computer device. Use of personal computer devices is strictly prohibited for remote access purposes unless approved by the Executive Director.

3. At no time should any Delaware County Intermediate Unit employee provide his or her login or email password to anyone, not even family members.

4. Only Information Management & Technology Staff-approved VPN software clients may be used.

Etiquette

The user, whether a student or employee, shall be subject to appropriate discipline, including, but not limited to, dismissal in the case of employees, and recommendation to home school district removal from an intermediate unit program in the case of students, in the event any one or more provisions of this policy is violated. In addition to disciplinary procedures, the user shall be responsible for the costs of damages to equipment, systems or software resulting from deliberate or willful acts. Illegal activities or use (for example, intentional deletion or damage to files or data belonging to others; copyright violations; etc.) may be reported to the appropriate legal authorities for possible prosecution. The Organization reserves the right to remove a user account from the network to prevent unauthorized or illegal activity.

Other Issues

The use of the Internet and email is a privilege, not a right. Organization administrative staff, along with the system administrator, will deem what is appropriate and inappropriate use, and their decision is final.

1. Disclaimer.

   The organization makes no warranties of any kind, whether express or implied, for the service it is providing. The organization is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruption. Use of any information obtained through the use of the organization's computers is at the user's risk. The organization disclaims responsibility for the accuracy or quality of information obtained through the Internet or email.

2. Charges.

   The organization assumes no responsibility or liability for any charges incurred by a user. Under normal operating procedures, there will be no cost incurred.

3. List Servers and Software.

   Subscriptions to list servers must be preapproved by the organization. A student may not download or install any commercial software, shareware, or freeware onto network drives or disks, unless he/she has the specific, prior written permission from an executive council member.

Antivirus

All Delaware County Intermediate Unit computers must have Delaware County Intermediate Unit's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Information technology department responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Delaware County Intermediate Unit's networks (e.g., viruses, worms, Trojan horses, email bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Acceptable Encryption

Proven, standard algorithms such as Triple DES, AES, RSA Security, Blowfish, and Twofish should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Delaware County Intermediate Unit’s key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Delaware County Intermediate Unit, Network Services. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Risk Assessment

To empower Information Management & Technology staff to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Risk assessments can be conducted on any entity within Delaware County Intermediate Unit or any outside entity that has signed a Third Party Agreement with Delaware County Intermediate Unit. Risk assessments can be conducted on any information system, to include applications, servers and networks, and any process or procedure by which these systems are administered and/or maintained.

The execution, development and implementation of remediation programs is the joint responsibility of Information Management & Technology staff and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Information Management & Technology Staff Risk Assessment Team in the development of a remediation plan.

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.[18][19]

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. Content shall be accessible to disabled users or available from another accessible source. 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

The network user 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 and/or intentional 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, 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. 47 CFR 54.520
16. 24 P.S. 1303.1-A
17. Pol. 237
18. Pol. 814
19. 17 U.S.C. 101 et seq

18 Pa. C.S.A. 2709

24 P.S. 4601 et seq

Pol. 220

Attachment Policy 815.docx (14 KB)