Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Number	815
Status	Active
Adopted	August 26, 1996
Last Revised	February 25, 2013

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.

In order to control the Total Cost of Ownership (TCO) of the information system, a number of standards and guidelines have been identified and are delineated as part of regulation 815A.

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

Access to the Internet - a computer or device shall be considered to have access to the Internet if the computer or device is equipped with a modem or is connected to a computer network which has access to the Internet.

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:[24]

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]

Collaborative technology - technology, files or documents whose main purpose is to facilitate collaboration via OJRSD IT Resources are considered shared data and files where the author and collaborator(s) have equal stakes in the creation and purpose of the files or documents.

Computer - includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.

Educational purpose/value - includes use of the system for classroom activities, professional or career development, and to support the district's curriculum, policy and mission statement. Entertainment or social-type activities, such as exchanging e-mail messages with friends, engaging in chat rooms, reading message boards, and other activities outside the scope of the user's education program, do not fall under the definition of educational value.

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:[1][2]

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:[25]

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.

Incidental personal use - use by an individual employee for occasional personal communications. Personal use must comply with this policy and all other policies, procedures and rules, and may not interfere with the employee's job duties and performance, with the system operations, or with other system users.

Internet - the Internet consists of multiple network services such as e-mail, web browsing, file transfer, and remote access.

IT Resources/OJRSD network - all components necessary to effect its operation, including, computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, software, and other computers and/or networks to which the district network may be connected, such as the Internet or those of other institutions. The network may also include virtual resources and services owned and managed by OJRSD and controlled by the design of the OJRSD infrastructure. The network does not include any foreign or rogue access to the Internet or resources considered external to the OJRSD network.

Minor - an individual who has not attained the age of seventeen (17).

Obscene - analysis of the material meets the following elements: whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; 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; and whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.[25]

Sexual Act and Sexual Contact - as defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3).[27]

Technology protection measure(s) - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[2]

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 Superintendent or his/her designee is responsible for the enforcement of this policy.

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.

This policy applies to all users of OJRSD computers, technology devices, network connectivity, and information technology resources. In addition, this policy applies to OJRSD Internet, computers/devices or network resources, and services used during OJRSD-sponsored events on campus (hereinafter IT Resources). Each user of IT Resources must agree to this policy, by signing a copy of the policy in hardcopy, prior to obtaining access to IT Resources. This policy applies to employees, consultants, volunteers, and any other persons obtaining access to IT Resources. Additionally, all students must obtain their parent's/guardian's signature to this policy granting permission to the student to use personal IT and district IT Resources during school hours or activities.

The Board declares that computer and network use is a privilege, not a right. IT Resources are the property of the OJRSD.

Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the OJRSD IT Resources, including personal files or any use of OJRSD IT Resources.

OJRSD 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 district's Internet, computers and network resources.

OJRSD additionally reserves the right to:

1. Determine which network services will be provided through IT Resources.

2. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through IT Resources, including e-mail.

3. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time (in accordance with Policy 800) and after notification to the user.[3]

4. Limit e-mail or file storage in an effort to preserve and manage fileserver disk space.

5. Log Internet and network use by students and staff.

6. Revoke user privileges, remove user accounts, and refer to legal authorities when violation of this and any other applicable district policies occurs or state and federal law is violated, including, but not limited to, those governing network use, copyright, security, discipline and vandalism of district resources and equipment.[4][5][6][7][8]

Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, inaccurate, obscene, profane, pornographic, offensive, and illegal, can be accessed through the network. Because of the nature of the technology that allows the Internet to operate, OJRSD cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of IT Resources and will result in suspension of network privileges and disciplinary action, as outlined in appropriate district policies.[4][5][6][7][8]

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: defamatory; lewd, vulgar, or profane; threatening; harassing or discriminatory; bullying; and terroristic.[2][9][10][11][12][13][14][15][16]

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.[17]

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 that may be used to track and recover lost or stolen equipment.

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.

Board policies on the selection of materials will govern the use of the Internet.

When using IT Resources for class activities, teachers will select material that is appropriate for the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

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 or designees 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:[1][2][18]

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:[2]

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

2. Cyberbullying awareness and response.[13][19]

Guidelines

The primary use of our IT Resources is reserved for those who need to access or obtain information and materials of educational value to them. **Educational value** means the information and/or materials must have a direct impact on the user's current education program in which s/he is enrolled or is seeking to enroll.

Users who use IT Resources for noneducational purposes may be responsible for any costs associated with such noneducational use. OJRSD may impose time restrictions on use of its IT Resources to ensure that all users have equal opportunity for use. OJRSD also may create and enforce storage management procedures or revise such storage procedures, at its option.

All users are obligated to be responsible custodians of the resources and services they create or to which they contribute via OJRSD IT Resources.

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 websites, etc.

Internet safety measures shall effectively address the following:[2][18]

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.

Exception to Filtering

Only the Superintendent or designee may provide a segregated or protected portion of the network or disable filtering technology or any other technology protection measure which OJRSD has placed on its computers. A user may not disable such technology.[1][17][20]

Any adult who desires to have such technology disabled must present a request in writing to the Superintendent or designee, and the Superintendent or designee will determine whether or not to grant the request. Any change in the technology will occur only for the purpose of enabling access by adults to the Internet to perform bona fide research or for other lawful purposes.

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. Nondistrict or nonschool related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.[13][19]
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.[21]
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.[22]
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.

Collaborative Technology

Access to technology, data or files authored or shared by any user, by authorized designees or the OJRSD administration are subject to the conditions of this policy.

OJRSD acknowledges that access to these documents or files may be subject to the rules and regulations provided by a third-party vendor whose main purpose is to provide OJRSD with the ability and capacity to use collaborative technology.

Security

System security is protected through the use of passwords and encryption. 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 Infringement

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.[22][23]

E-Mail and Communications

The use of e-mail, as a communications medium, should not be used to solicit or proselytize others for commercial ventures, religious or political causes, outside organizations, or other nonschool district related solicitations. Students are only permitted to use e-mail or e-mail services provided by OJRSD.

All internal communications and information accessible via OJRSD IT Resources shall be assumed to be district property and shall not be disclosed except for school district purposes consistent with the objectives of this policy.

All computer communication systems, and all communications and stored information transmitted, received, or contained in the OJRSD information systems are the property of OJRSD and are to be used primarily for educational purposes. All e-mail messages are OJRSD-owned messages/data. To ensure proper use of computer systems and equipment, OJRSD may monitor the use of these systems and equipment from time to time. Such monitoring may include, but not be limited to, entering a staff member’s e-mail files whenever there is a school district business need to do so.

Network Availability

OJRSD may terminate the availability of the network or the Internet in its sole discretion.

Device Management

Through the use of device management resources and services, OJRSD may know the approximate location of any OJRSD-owned device based on the device's ability to access a wireless repeater whenever it is active. This location information may be used for aggregate reporting or tracking should the device be removed from the OJRSD campus.

District Website

The district shall establish and maintain a website 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 website shall comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.

Search and Seizure

User violations of the district Acceptable Use Policy, the Student Disciplinary Code, district policy or the law may be discovered by routine maintenance and monitoring of the district system, or any method stated in this policy, or pursuant to any legal means.

OJRSD employees should be aware that their personal files very well may be discoverable and could be discoverable in the event of any form of litigation.

Everything that OJRSD employees place in their personal files should be written as if a third party would review it.

In no event shall OJRSD be liable to any staff member for any damages, whether direct, indirect, special or consequential, arising out of the use of the Internet, accuracy or correctness of data bases or information contained therein or related, directly or indirectly, to any failure to delay of OJRSD in providing access to the Internet.

Consequences for Inappropriate Use

Users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[17]

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 as determined by OJRSD or student handbook, and/or legal proceedings.[4][5][6][7][8]

Warranty

OJRSD makes no warranties of any kind, either expressed or implied, that the functions or the services provided by its network will be error-free or without defect. OJRSD does not warrant the effectiveness of Internet filtering.

The electronic information available to users does not imply endorsement of the content by OJRSD, nor is OJRSD responsible for the accuracy or quality of the information obtained through or stored on the network.

OJRSD shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, or unavailable when using the computers, network, and electronic communication system.

OJRSD will not be responsible for material that is retrieved through the Internet or the consequences that may result from them.

OJRSD will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the OJRSD network.

In no event will OJRSD be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the network.

Legal

1. 20 U.S.C. 6777
2. 47 U.S.C. 254
3. Pol. 800
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. 218.2
13. Pol. 249
14. Pol. 348
15. Pol. 448
16. Pol. 548
17. 24 P.S. 4604
18. 47 CFR 54.520
19. 24 P.S. 1303.1-A
20. 24 P.S. 4610
21. Pol. 237
22. Pol. 814
23. 17 U.S.C. 101 et seq
24. 18 U.S.C. 2256
25. 18 Pa. C.S.A. 5903
26. 18 Pa. C.S.A. 6312
27. 18 U.S.C. 2246

24 P.S. 4601 et seq