

# Acceptable Use Of Internet, Computers and Network Resources

## **Purpose**

The School District of Philadelphia provides students, staff and other authorized individuals with access to computing equipment, electronic communication systems and network resources, which includes Internet access, whether wired or wireless, or by any other means. This access has a limited education purpose for students and is to facilitate employees' work productivity

For instructional purposes, the use of Internet, computers and network resources 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**

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. 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.

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. 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:

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.

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.

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

### **Authority**

The district has the right to place restrictions on the use of equipment, resources and material users access or disclose through the district's Internet, computers and network resources. Users are expected to follow School Reform Commission policies and administrative procedures governing conduct and discipline, and law and

regulations, in their use of the district's Internet, computers and network resources. This access has not been established as a public access service or a public forum.

All district employees and students shall have access to the Internet through the district's private network. Parents/Guardians may specifically request that their children not be provided such access by notifying the district in writing.

The district makes no guarantee that the functions or the services provided by or through the district Internet, computers or network resources will be error-free or without defect. The district is not responsible for any damage suffered, including, but not limited to, loss of data or interruptions of service.

The district is not responsible for the accuracy or quality of the information obtained through or stored on the Internet or network resources. The district shall not be responsible for financial obligations arising through the unauthorized use of the Internet or network resources.

The SRC declares that computer and network use is a privilege, not a right. The district's computer and network 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, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor filespace 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 Providers (ISPs), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.

Users must utilize the district's wired and wireless networks for access to the Internet in school district schools and facilities. No other method or means of access (i.e. USB modem, MiFi router, personal Internet access, open WiFi networks, etc.) is permitted while connected to a district network or while using a district technology resource.

The SRC requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

#### Filtering/Inappropriate Material

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established policy, or the use of software and/or online server blocking. Specifically, as required by law and in recognition of the need to establish a safe environment, 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.

The SRC authorizes the Superintendent or designee to establish a list of materials that are inappropriate for access by users, which shall include but not be limited to:

1. Obscene.
2. Child pornography.
3. Harmful to minors.
4. Other materials prohibited by law or this policy.

Upon request by staff, the Filtering Review Committee 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, in accordance with applicable law.

### **Delegation of Responsibility**

The district shall make every effort to ensure that students and staff use this resource responsibly.

The district shall inform staff, students, parents/guardians and other users about this policy through posting on the district web site and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.

By accessing the district's Internet, computers and network resources, users acknowledge awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and may use tracking systems to track and recover lost or stolen equipment.

The Chief Information Officer shall be responsible for the development, publication, implementation and ongoing administration and enforcement of the procedures, processes and techniques required to protect the district's technology systems and services from unauthorized access, loss or misuse.

School principals have the responsibility to establish a plan to ensure adequate supervision of students and are also responsible for interpreting and enforcing this policy at the local level.

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.

The Superintendent or designee shall be responsible for recommending technology and developing procedures and plans 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. 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 SRC.
2. Maintaining and securing a usage log.
3. Monitoring online activities of minors.

The Superintendent or designee shall develop and implement administrative procedures that ensure students are educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking web sites and in chat rooms.
2. Cyberbullying awareness and response.

## **Guidelines**

### E-Mail

The district provided e-mail is the official e-mail of record for the district and should be used for all official business.

Users shall not post, advertise or disclose for public viewing in either print or electronic form, the e-mail address of any person or persons without their explicit permission.

Students shall not be given access to district-provided e-mail.

Guests/Contractors are not automatically eligible for a district e-mail account. E-mail or network access accounts may be granted if directly sponsored by a district administrator.

All electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of e-mail are

the property of the district. E-mail messages are considered to be district property and may be retrieved, if necessary, from individual computers even though deleted by the sender and receiver. E-mail communications that qualify as district records shall be maintained in accordance with applicable policy, administrative procedures and/or retention schedule(s).

Use of the district e-mail system is subject to all applicable laws, regulations and policies.

### 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, unwelcome or inappropriate 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 chat rooms, e-mail, social networking web sites, etc. Personal information includes, but is not limited to, name, e-mail address, home address, telephone number, school address, work address, pictures or video clips.

Internet safety measures and administrative procedures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using e-mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online disclosures or 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 and procedures, accepted rules of network etiquette, and federal and state law and regulations. Specifically, the following uses are prohibited:

1. Users shall not use the district's Internet, computers or network resources to access, send, receive, transfer, view, share, or download material that is profane, obscene, pornographic, advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).
2. Students shall not agree to meet with someone they have met on the Internet without their parent's/guardian's approval and participation.
3. Users shall not attempt to gain unauthorized access to any computer system or network. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of browsing, snooping, or electronic discovery.
4. Users shall not deliberately disrupt or harm hardware, systems or files; interfere with computer or network performance; interfere with another's ability to use equipment and systems; or destroy data.
5. Users shall not use the district's Internet, computers or network resources to engage in illegal acts, such as arranging for a drug sale or the purchase of alcohol; engaging in criminal gang activity; threatening the safety of persons; and accessing, sharing, distributing or reproducing unauthorized copyrighted materials.
6. Users shall not utilize peer-to-peer file sharing applications or execute programs to facilitate the downloading or exchange of copyrighted or unauthorized materials.
7. Users shall not use the district's Internet, computers or network resources to solicit information with the intent of using such information to cause personal harm or bodily injury to another or others.
8. Users shall not post or distribute information that could endanger an individual, cause personal damage or cause service disruption.
9. Users shall not knowingly or recklessly post false or defamatory information about a person or organization.
10. Users shall not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users.
11. Users shall not indirectly or directly make network connections that create backdoors to the district, other organizations, community groups, etc., that allow unauthorized access to the district's network.
12. Users shall not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening or disrespectful language.

13. Users shall not engage in personal attacks, including prejudicial or discriminatory attacks.
14. Users shall not harass another person.
15. Users shall not repost or distribute a message that was sent to them privately without the permission of the person who sent the message.
16. Users shall not forward or post chain letters or engage in spamming. Spamming is sending an annoying or unnecessary message to a large number of people.
17. Users shall not install, use or reproduce unauthorized or unlicensed software on district resources.
18. Users shall not plagiarize works that they find on the Internet or other resources.
19. Users shall not use district Internet, computers, or network resources for private business activities, commercial or for-profit purposes, product advertisement, or unreasonable personal use.
20. Users shall not use the district's Internet, computers, or network resources for political lobbying.
21. Students shall not download files unless approved by their teacher.
22. Users shall not engage in bullying/cyberbullying.
23. Students shall not access material that is harmful to minors or is determined inappropriate for minors in accordance with SRC policy.
24. Users shall not transmit material likely to be offensive or objectionable to recipients.
25. Users shall not engage in impersonation of another user, anonymity, and pseudonyms.
26. Users shall not disable or bypass the Internet blocking/filtering software without authorization. This includes, but is not limited to, the use of proxy avoidance type software and hardware as well as filesharing software.
27. Users shall not access, send, receive, transfer, view, share or download confidential information without authorization.

28. Users are prohibited from directly registering or obtaining Internet domain names, Internet address space, security certificates or other related Internet services on behalf of or representing any school, administrative office or the district as a whole.

29. Users may not acquire, contract with, or utilize unauthorized technology-based software, hardware or external hosting services on behalf of or representing any school, administrative office or the district as a whole.

### Security

Use of employee ID numbers (EIDNs) and Social Security numbers (SSNs) shall be in accordance with SRC policy and administrative procedures.

Users are responsible for the use of their individual access account(s) and should take all reasonable precautions to prevent others from being able to use their account(s), including coworkers, friends or family.

Every user ID, system account and application account must be authenticated with a password. System security is protected through the use of passwords. Failure to adequately protect or update passwords in accordance with established procedures could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed:

1. Users 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. Every account shall be limited to one (1) active session at a time.
4. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.
5. Unauthorized attempts to log on to the district's network or any other network as a system administrator is prohibited.
6. Users should immediately notify a teacher or system administrator of any possible security problem.

### 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.

### Consequences For Inappropriate Use

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

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, and/or legal proceedings, in accordance with applicable law, regulations and SRC policies.