Oklahoma City Public Schools

Acceptable Use Policy (AUP)

Student Computer & Network Access Wireless Devices

Computer and Network access is a privilege provided for District students and staff for the sole purpose of facilitating resource sharing and communication. Students are to only use these services for legitimate educational purposes under the supervision of school personnel. Students are provided login information with an individual user name or ID and password that is computer generated to access the computer and network. Students are to never share their login information with anyone. Students are required to logout when finished accessing the network.

The District is not responsible for the misuse of online services. Such misuse includes, but is not limited to; obtaining inappropriate or sexually explicit material, illegal copying or installation of software, using another's password, producing, copying, or attempting to introduce any computer code designed to self-replicate, damage, or destroy a computer's memory, cause a virus, or otherwise hinder computer performance. Students found guilty of such behaviors are subject to the loss of computer privileges and action as stated in the Student Code of Conduct guidelines. It will not be a defense to any disciplinary consequence for a student to say someone else used their account, or the student forgot to log out.

For reasons of health and safety, school staff may periodically monitor each student's use of the network resources to insure that the system is being used in accordance with district policy. Students who lose their individual computer or network privilege will still be required to complete any district or state online testing. Please contact your school's office or the district technology IT Services helpdesk at 587- 4357 with further questions.

Students may possess a wireless telecommunications device while on school premises, or while in transit under the authority of the school, or while attending any function sponsored or authorized by the school. Use of such wireless communication devices by students during the instructional day for educational purposes only is at the teacher's discretion. The instructional day shall be defined as including all times when classes are being conducted and during passing times. Wireless telecommunication devices include, but are not limited to, cellular and digital telephones, two-way radios, personal digital assistants, and smartphones. Wireless telecommunication devices do not include amplification systems utilized in classrooms or in school buildings.

Students found to be using any electronic communications device for any illegal purpose, cyberbullying, threatening others, violating privacy, or to in any way send or receive personal messages, data, or information that would contribute to or constitute cheating on tests or exams shall be subject to discipline and the device shall be confiscated and will be returned to the parent during a parent conference. Students violating this rule will be disallowed from carrying a personal communication device following the incident unless a bona fide health emergency exists. Where appropriate, police authorities may be contacted. OKCPS is not responsible for personal wireless telecommunication devices.

1. Introduction

Computer network resources, provided by the Oklahoma City Public Schools, enable communication with electronic communities around the world. These computer network resources include Internet, e-mail, the student enterprise system, and the business enterprise systems. The use of these electronic resources shall be consistent with the purpose, mission, and goals of the Oklahoma City Public Schools and used only for the educational and professional purposes. The purpose in providing these services is to facilitate access to information and resources, promote educational excellence, and enhance communication between schools, offices, regional education service centers, and other worldwide educational entities.

The Internet is a network connecting thousands of computers throughout the world. The Internet can bring a wealth of educational material to the classroom, but may also contain material that is objectionable. The Oklahoma City Public Schools filters web sites, chat rooms, instant messengers, and some emails believed to be inappropriate for students, teachers, administrators and staff. However, no filtering system is perfect. The District cannot and does not represent that inappropriate or objectionable material can be completely filtered. Parent(s) and guardian(s) must consider this in deciding whether to permit their children access to the District's computer network resources. This Acceptable Use Policy (AUP) is provided so that staff, students, and members of the community using the District's computer network resources are aware of their responsibilities. The use of these network resources is a privilege, not a right. Any violation of these policies will result in the loss of network privileges as well as possible disciplinary action.

2. Access to District Network Resources

- All employees must sign an Acceptable Use Policy agreement when hired and on a yearly basis before access is granted to the District's computer network resources. If an employee objects to signing an AUP they will not be allowed on the district network which could affect their employment status.
- Staff, students, and members of the community may be given access to the District's computer network resources. This access, including account and password, must not be shared, assigned, or transferred to another individual.
- Access to the District's computer network resources may be suspended or terminated if terms and conditions of this AUP are violated. Prior to a termination of access to the District's computer network resources, the user will be informed of the suspected violation and given an opportunity to present an explanation. The user may request a review hearing with an appointed hearing officer within seven (7) days of notification if the user feels that such action is unjust. After the review, access may be terminated if the hearing officer denies the appeal as well as disciplinary consequences deemed appropriate by the school administrator.

3. System Security

- Computer users may not run applications or files that create a security risk to the District's computer network resources. If users identify a security problem, they must notify appropriate administrators immediately.
- Any user deemed to be a security risk, or discovered to have a proven history of problems with other computer networks, may be denied access to the District's computer network resources.
- Users should immediately notify Information Technology if they believe that someone has obtained unauthorized access to their private account.

4. Respecting Resource Limits

- Staff, students, and community members will not post chain letters or engage in spamming. Spamming is sending unsolicited "junk" messages to a large number of people, or sending a large number of messages to a single person, with the intent of annoying users or to interrupt the system.
- The system administrators reserve the right to set a limit on disk storage for network users as well as blackmail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses.
- Advertising will be permitted on the District's computer network resources with the prior approval of the appropriate administrator.

5. Illegal Activities

- The District will cooperate fully with local, state, or federal officials in any investigation related to illegal activities that blatantly corrupt the educational value of computers or instances that violate the law.
- Attempting to gain unauthorized access to the District's network resources or go beyond authorized access is prohibited. This includes attempting to log in through another person's account or accessing another person's files.
- Vandalism will result in cancellation of privileges to the District's computer network resources. Vandalism is defined as any malicious attempt to harm or destroy data or equipment on any computer network.
- It is prohibited to use the District's computer network resources with the intent of denying others access to the system.

6. Intellectual Property (Copyright)

- No copyrighted material is to be placed on the District's computer network resources without written permission from the copyright owner.
- Any material placed on the District's network or web pages by an employee, with the use of district or personnel technology will become property of the District unless permission to keep Intellectual Property rights is granted in writing by the employee's supervisor or the Information Technology Department.
- All users of the District's network resources must agree not to submit, publish, or display any type of material that violates this AUP.

7. Software

Only software approved (certified) by the Information Technology's Technology Purchase Request (TPR) review committee and proof of valid software license(s) can be used on District computer systems including freeware, shareware and beta/test software.

Software that is damaging to the District's network resources or any other systems is prohibited.

8. Digital Citizenship

- Polite and appropriate language is expected at all times. Abusive messages are prohibited.
- Harassment is unacceptable and prohibited. Harassment is conduct, which is sufficiently severe, persistent, or pervasive that it adversely affects, or has the purpose of logical consequence of interfering with a user's educational program, or creates an intimidating, hostile, or offensive environment. Behavior that continues after an individual is informed of its offensiveness may constitute evidence of intent to harass. If told by a person to stop sending messages, the sender must stop.
- Cyberbullying is prohibited. This includes, but is not limited to, the following forms: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, digital pictures or images, or website postings (including blogs or social media sites), which has the effect of physical or emotional harm. Anyone who engages in such activity is in violation of this policy and shall be subject to appropriate discipline.

- Teachers will be provided curriculum for educating students about digital citizenship and appropriate and safe online behavior, including interacting with others using social networking and chat rooms and how to properly address cyberbullying situations. They will be provided information created by the district's Educational Technology training team for reference and use in instruction.

9. Liability

- Oklahoma City Public Schools does not warrant the functions or services performed by the District's computer network resources. Resources are provided on an "as is, as available" basis.
- Opinions, advice, services and all other information supplied by third parties are for informational purposes only. It is not guaranteed to be correct. Users are urged to seek professional advice for specific individual situations.
- Any software available from the District's network resources is not guaranteed as to suitability, legality, or performance by Oklahoma City Public Schools.
- Staff, students and community members agree to indemnify and hold harmless Oklahoma City Public Schools for any liability arising out of any violation of this AUP.

10. Electronic Mail and Real-Time Conferencing

- It is not the intention of the Information Technology Department to inspect or disclose the contents of electronic mail or computer files sent by one user to another, without consent from either party, unless required to do so by Oklahoma City Public Schools, local, state or federal officials. Electronic mail is not private. As with written communications, users should recognize there is no expectation of privacy for electronic mail.
- Users are expected to remove e-mail messages in a timely manner.
- All users must promptly report inappropriate messages received to a teacher, supervisor, or the system administrators. Any user should not reveal personal information such as addresses, phone numbers, passwords, or financial information to others. Private information may not be posted about another person. Individuals need to use caution when corresponding or communicating through email, chat rooms, instant messengers or websites.
- A canceled account will not retain electronic mail.
- The system administrators reserve the right to terminate access to the District's computer network resources if this AUP is violated while using electronic mail and real-time chat features, including video conferencing.
- While we allow personal e-mail to be sent through the system, please remember that this account is for work/school purposes, and all mail (and other data) residing on the Network is the property of Oklahoma City Public Schools. We highly discourage subscribing to personal mailing lists and using your network account for promotions, giveaways, sweepstakes, and other non-business related communications. Excessive amounts of mail received from such sources may be deleted without warning. Any mail that is related to running a private business or involved in unsolicited advertising will be deleted and its sender's e-mail privileges may be revoked. Similarly, the Oklahoma City Public School district does not permit the "relaying" of e-mail. Mail relaying is when mail is sent from an outside account through Oklahoma City Public Schools' e-mail server for the purpose of masking who the original sender was.
- Abusing District distribution lists is prohibited. Examples of abusing a distribution list include sending mail to the entire District to inform all users of the system that your child is selling candy and to see you for details. This kind of solicitation unnecessarily clogs the email system and frustrates users. Electronic mail is an efficient and convenient means of communication, but problems can arise when it is used without restraint and discipline.

Other prohibited electronic communications include, but are not limited to:

- Using another's password.

- Use of electronic communications to send copies of documents in violation of copyright laws;
- Use of electronic communication systems to send messages, access to which are restricted by laws or regulations;
- Capture and "opening" of undeliverable electronic communications except as required in order for authorized employees to diagnose and correct delivery problems;
- Use of electronic communications to intimidate others or to interfere with the ability of others to conduct District business.
- "Spoofing," i.e., constructing electronic communications so it appears to be from someone else;
- "Snooping," i.e., obtaining access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial District business purpose;
- Attempting unauthorized access to data or attempting to breach any security measures on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.
- Sending or displaying offensive messages or pictures; using obscene language.

11. Consequences

Financial and criminal penalties may be incurred by Oklahoma City Public Schools for pirated or unlicensed software. These penalties may be passed on to the offender. Software piracy and license fraud is a serious crime and results in extraordinarily high fines (usually twice the value of the pirated software title). If user is unclear of such software, contact the Information Technology Department.

Violation of Oklahoma City Public Schools' policies, regulations and procedures concerning the use of the WAN and the Internet will result in the same disciplinary actions that would result from similar violations of other Oklahoma City Public School policies and/or regulations. Any or all of the following consequences may be employed:

- Any campus-based disciplinary consequence, including suspension, deemed appropriate by the school administration.
- Long-term suspension may be considered in flagrant violations that blatantly corrupt the educational value of computers or in instances when users have used Oklahoma City Public Schools' WAN or Internet access to violate the law or to compromise the relationship between Oklahoma City Public Schools and our ISP.
- Employees found to be using the WAN or Internet access inappropriately or illegally are subject to progressive disciplinary consequences specified under applicable Board policies/regulations or negotiated agreements.