

## **Electronic Communications System**

### 1. Purpose

- a. The purpose of the district network is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people from throughout the world. Additionally, the system will be used to increase district intracommunication, enhance productivity, and assist district employees in upgrading their skills through greater exchange of information with their peers. The district network will also assist the district in sharing information with the local community, including parents, social service agencies, government agencies, and businesses. The district network is limited to educational uses. Occasional personal use is permitted, but this use will be treated no differently from use relating to the district's business.
- b. The district will provide employees and students with access to the district's electronic communication network for educational purposes and professional communication. This network includes local area networks in each facility (LAN), communications between all of the district's local area networks, and Internet access.
- c. Users may not use the district network for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for district purchase of goods or services through the district network.
- d. The term "educational purpose" includes use of the network for classroom activities, research, and professional development.

### 2. District Responsibilities

- a. The superintendent or designee will serve as the coordinator to oversee the district network and will work with the district technology committee, school site councils, and administrators as well as with other regional or state organizations.
- b. The superintendent will establish administrative regulations for use of the district's system by staff using their own personal electronic devices to download and store district proprietary information including personally recognizable information about the district students or staff. Regulations shall insure compliance with privacy rights under applicable federal and state laws and regulations, including but not limited to the Age Discrimination in Employment Act of 1967 (ADEA), the Americans with Disabilities Act (ADA), the Genetic Information Nondiscrimination Act of 2008 (GINA) and the Health Insurance Portability and Accountability Act of 1996 (HIPPA).
- c. The district technology committee, made up of school representatives and coordinated by the superintendent or designee, will serve as the clearing house for technology related issues and

will make recommendations to the administrative team for policy changes as needed. The committee will meet on a regular basis throughout the year.

- d. The superintendent or designee will establish processes for establishing access and necessary account limits for the district network. This may include, but is not limited to setting up individual and class accounts, setting quotas for disk usage, and establishing a retention schedule.

### 3. Access to the System

- a. The district's Acceptable Use Policy and Agreement, state and federal law, the Children's Internet Protection Act, and regulations in the Student Handbook will govern all use of the district network. State and federal law, district policy, the Collective Bargaining Agreement(s), and the district's Acceptable Use Policy and Agreement will govern employee use of the network.
- b. The superintendent will establish administrative regulations for the use of the district's system, including compliance with the following provisions of the Children's Internet Protection Act:
  - (1) Technology protection measures, installed and in continuous operation, that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to the use of the computers by minors, harmful to minors.
  - (2) Monitoring the online activities of minors.
  - (3) Denying access by minors to inappropriate matter on the Internet and World Wide Web.
  - (4) Ensuring the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.
  - (5) Prohibiting unauthorized access, including so-called "hacking" and other unlawful activities by minors online.
  - (6) Prohibiting unauthorized disclosure, use and dissemination of personal information regarding minors.
  - (7) Installing measures designed to restrict minors' access to materials harmful to minors.

The administrative regulations will be consistent with sound guidelines as may be provided by the education service district, the Oregon Department of Education and/or the Government Standards and Practices Commission and will include a complaint procedure for reporting violations.

Failure to abide by district policy and administrative regulations governing use of the district(s) system may result in the suspension and/or revocation of system access. Additionally, student violations will result in discipline up to and including expulsion. Staff violations will also result in discipline up to and including dismissal. Violations of law will be reported to law enforcement officials. Fees, fines or other charges may also be imposed.

### 4. Parental Notification and Responsibility

- a. The district will notify parents about the district network and the policies (e.g., filtering) governing its use.

Parents will receive notification about the district network and policies governing its use during school registration. Students will be allowed access to the Internet without parent signature. If a parent objects to their child having access to the district network, the parent must notify the school principal by completing and signing a Denial of Access Form available from school offices. The Acceptable Use Policy is to be included in the student handbook.

Parents may request alternative activities for their child(ren) that do not require self-directed individual Internet access.

- b. Parents have the right at any time to investigate the contents of their child(ren)'s computer or E-Mail files. The district will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the district network. Parents have the right to request the termination of their child(ren)'s individual account at any time.
- c. The district Acceptable Use Policy and Agreement contains restrictions on accessing inappropriate material. The district will provide students and parents with guidelines for student safety while using the Internet.

#### 5. District Limitation of Liability

- a. The district makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruption of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.
- b. The district assumes no responsibility for unintended disclosure of personal information to unauthorized persons that may result through accident, unauthorized use, or inappropriate use of the system. Each person using the system assumes the risk of the possibility that their expectation of privacy may be breached, notwithstanding use of appropriate security measures.
- c. The district assumes no responsibility for damage to or loss of hardware, software or stored information by an individual accessing the district network with personal computing device(s). Each person using personal computing devices (with or without permission) on the district network assumes all risks associated with that use. This includes both wireless and wired access.

#### 6. Due Process

- a. The district will cooperate fully with local, state, and federal officials in any investigation concerning or relating to any illegal activities conducted through the district network.
- b. In the event a student violates the district's Acceptable Use Policy and Agreement, the student may be disciplined pursuant to the procedures described in state and federal law and/or the Student Handbook.
- c. Employee violations of the district Acceptable Use Policy and Agreement will be handled in accordance with state and federal law, district policy, and the Collective Bargaining Agreement(s).

## 7. Search and Seizure

- a. Students and district employees should use caution to avoid unauthorized disclosure of confidential information of all kinds including, but not limited to, student records (as defined by state and federal law) and personnel information when using the district's electronic communications network.
- b. It is the responsibility of every user of the system to report immediately to the building principal, the district superintendent, or his designee any known or suspected unauthorized use, inappropriate use, breaches of established system security, or violation of required system use procedures.
- c. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating state and federal law, the district Acceptable Use Policy and Agreement, regulations in the Student Handbook, and district policy.
- d. An individual search of computer records and files may be conducted if there is reasonable suspicion that a user has violated state and federal law, regulations in the Student Handbook, or district policy. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

## 8. Copyright and Plagiarism

- a. District policies on copyright will govern the use of material accessed through the district network. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.
- b. District policies on plagiarism will govern use of material accessed through the district network. Teachers will instruct students in appropriate research and citation practices.

## 9. Academic Freedom, Selection of Material, Student Rights to Free Speech

- a. Board policies will govern the use of the district electronic communications network.
- b. When using the Internet for class activities, teachers will select material that is relevant to the course objectives. Teachers will provide guidelines to assist their students in channeling their research activities effectively and properly.

## 10. District Acceptable Use Policy and Agreement

The district will develop regulations guiding acceptable use of the network directed toward personal safety, illegal activity, system security, inappropriate conduct, respecting resource limits, limited expectation of privacy, plagiarism, copyright infringement, and inappropriate access to material.

END OF POLICY

---

**Legal Reference(s):**

[ORS 30.765](#)  
[ORS 133.739](#)  
[ORS 163.435](#)  
[ORS 164.345](#)  
[ORS 164.365](#)  
[ORS 167.060](#)  
[ORS 167.065](#)  
[ORS 167.070](#)

[ORS 167.080](#)  
[ORS 167.087](#)  
[ORS 167.090](#)  
[ORS 167.095](#)  
[ORS Chapter 192](#)  
[ORS 332.107](#)  
[ORS 336.222](#)

[ORS 339.250](#)  
[ORS 339.270](#)  
  
[OAR 581-021-0050](#)  
[OAR 581-021-0055](#)  
[OAR 584-020-0040](#)  
[OAR 584-020-0041](#)

Children’s Internet Protection Act, 47 U.S.C. Sections 254 (h) and (l) (2008); 47 CFR Section 54.520 (2001).  
Copyrights, Title 17, as amended, United States Code; 19 CFR Part 133 (2000).  
*Oregon Attorney General’s Public Records and Meetings Manual*, pp. 24-26, Appendix H, Department of Justice (2001).  
Safe and Drug-Free Schools and Communities Act, 20 U.S.C. Sections 7101-7117.  
Drug-Free Workplace Act of 1988, 41 U.S.C. Sections 701-707; 34 CFR Part 85, Subpart F.  
Controlled Substances Act, 21 U.S.C. Section 812, schedules I through V, 21 CFR 1308.11-1308.15 (2000).  
Drug-Free Schools and Communities Act Amendments of 1989, P.L. 101-226, 103 Stat. 1928.  
Americans with Disabilities Act of 1990, 42 U.S.C. Sections 12101-12213; 29 CFR Part 1630 (2000); 28 CFR Part 35 (2000).  
Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232g; 34 CFR Part 99 (2000).  
Oregon Government Standards and Practices Commission, Advisory Opinion No. 98A-1003 (July 9, 1998).  
No Child Left Behind Act of 2001, P.L. 107-110, Title II, Section 2441.  
Americans with Disabilities Act Amendments Act of 2008.

**Cross Reference(s):**

GBNAA/JFCFA - Cyberbullying  
IIBGB - Web Pages