Lake County School District 7

Code: **GBP**
Adopted: 8/28/06
Readopted: 3/28/11
Orig. Code(s): GBP

Employee Access to District Electronic Communications Systems

It is the policy of the Board to provide district employees access to a computer network that is designed, purchased and maintained to support the programs and operations of the district. The Board anticipates that faculty and administration will design and implement the use of pedagogically sound electronic information resources and activities throughout the curriculum in order to enhance instruction and aid learning. Faculty and building-level administration shall select these networked electronic resources with the same care and scrutiny as with any other approved text, print, video or audio material. Employees are to be advised that all use of the district's network is public in nature and subject to review by designated personnel. Employees shall be held accountable to good behavior on the network just as they are by professional standards of ethical behavior in all aspects of their job performance. It is not the purpose, nor is it intended that employees use the district's computer network system for personal benefit or gain; or for the conveyance of confidential communications on students or employees.

Access to the district's information resource system will be governed in accordance with the following requirements:

1. Resource/Program Development: The superintendent shall develop and maintain districtwide practices and procedure used to approve technological resources placed on the network for staff. Approved resources shall be justified as to how they apply to and improve the educational, support and administrative functions of the district. The procedure shall ensure that district-level staff have reviewed and evaluated each technology request for system compatibility and serviceability prior to budget proposals, purchase and use;

2. Children's Internet Protection Act: The superintendent shall develop districtwide practices and procedures to ensure compliance with the following provisions of the Children's Internet Protection Act:

    a. 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;
    b. Monitoring the online activities of minors;
    c. Denying access by minors to inappropriate matter on the Internet and World Wide Web;
    d. Ensuring the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
    e. Prohibiting unauthorized access, including so-called "hacking" and other unlawful activities by minors online;
    f. Prohibiting unauthorized disclosure, use and dissemination of personal information regarding minors;
    g. Installing measures designed to restrict minors' access to materials harmful to minors.

3. Policy Distribution/Use Agreement: As part of the annual fall in-service, or otherwise upon employment, employees shall be given copies of this policy and policy IIBGA – Student Access to Networked Information Resources. All employees shall have on file a signed "Acceptable Use Agreement" indicating they have received, read, understand and will comply with these policies. This agreement shall be on file prior to the network administrator establishing the employee's account on the network;

4. Network Rules: Employees shall be held responsible to a level of behavior on the school's computer network that is consistent with this policy in compliance with professional standards as outlined in Oregon Revised Statutes and administrative rules, and, by the district's expectation of ethical behavior by employees in all aspects of their job performance.

   Some aspects of computer network access and operation (e.g., communication and attendance) may be deemed a requirement of employment; others (e.g., Internet and E-mail) a privilege; and still others (e.g., payroll and leave accounting) a prohibited activity for most employees. The computer network, its hardware, software and its telecommunications capabilities are to be used as intended by employees for approved instructional purposes and to further support the programs and operations of the district.

5. Public Records Law: Because conveyance of confidential communications concerning employees and students is prohibited by this policy on the district's system, all employee use (both sent and received) is a "public record". Though generally secure from the scrutiny of students, staff and patrons, employees shall be notified that at no time should they consider the system to be private or secure. Designated staff shall have the responsibility to review files and communications to maintain system integrity and ensure that employees are using the system ethically and responsibly;

6. Retention of E-mail: Because the district is a public employer, employee E-mail (as it relates to the public records law) shall be retained as required by OAR Chapter 166 of the State Archivist and must be made available to the public, if requested. Routine, reading and chronological communications by employees will automatically be retained, as needed, in an electronic file, by the district's system, with no action necessary on the part of individual employees. Policy and historical communications, however, shall be printed in hard copy and stored permanently. Likewise, financial correspondence shall be printed in hard copy and be retained in accordance with applicable provisions of OAR 166-408-0010. Records enclosed or attached to E-mail shall have the same retention requirements as the record to which it is attached or enclosed;

7. Network Prohibitions: Because of the complexity, importance and interdependence of the district's computer network with the daily administration and execution of all phases of district operations, (instruction, support, administration, finance and maintenance) employees shall be subject to disciplinary measures and held liable for any inappropriate or harmful conduct or activity performed on the school's network. Employee prohibitions on the use of this system shall include, but are not necessarily limited to, the following:

   a. Conveying confidential communications regarding staff or students;
   b. Utilizing "nonapproved" disks (because of the probability of introducing a "virus");
   c. Using or installing unapproved or "pirated" software or programming applications;
   d. Connecting or docking unauthorized personal computers or other devices to the network;

e. Altering or manipulating system and/or machine configuration, protocol or programming;
f. "Pirating" or violating regulations and license agreements for district-purchased software;
g. Intentionally altering, disrupting or destroying system and/or machine capabilities;
h. Sending, retrieving or displaying offensive messages, pictures or video material, including any text file or picture or engaging in any communication that includes material which may be interpreted as:

(1) Harmful to minors;
(2) Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district;
(3) A product or service not permitted to minors by law;
(4) Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others;
(5) A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
(6) Defamatory, libelous, reckless or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense or otherwise violates any law, rule, regulation, Board policy and/or administrative regulation.

i. Sending/returning e-mail that is inconsistent with public education purposes;
j. Communications or activities intended to annoy, harass, insult or degrade others;
k. Communications or activities regarding political issues or candidates;
l. Communications relating to the operation of employee unions;
m. Activities and communications which violate separation of church and state rules;
n. Violation or misapplication of federal copyright laws;
o. Using the passwords of other students or employees;
p. Divulging system passwords and procedures to persons not entitled to use them;
q. Trespassing into unauthorized programs, applications, work or files of students or staff;
r. Knowingly and intentionally destroying public records as it pertains to the network;
s. Knowingly and intentionally wasting or misusing district resources and property; and
t. Utilizing the network for unauthorized commercial purposes, or for personal financial gain.

8. Disciplinary Sanctions: Depending on the severity and consequences of an employee's action, inappropriate use, misuse and/or abuse of the district's computer network by employees may result in disciplinary action including, but not limited to:

a. Verbal warning;
b. Written reprimand;
c. Restricted use/access to the network and its components;
d. Temporary loss of certain access rights to the network;
e. Permanent loss of certain access rights to the network;
f. Administrative leave with or without pay;
g. Termination from employment;
h. If appropriate, as required by law, referral to the Teacher Standards and Practices Commission for action;
i. If a law has been violated, referral to law enforcement agencies for legal action; and

j. Financial liability for costs incurred by the district in correcting and replacing the network's administrative protocol, programming, software, files and/or equipment if intentionally and knowingly disrupted, damaged, destroyed or misused by an employee.

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 339.260
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.