

300 PERSONNEL, continued

334 Electronic Communications Systems Acceptable Use

The Board of Directors recognizes electronic mail (e-mail), Internet, voice mail systems, video broadcast and video conferencing are all communications tools, which are effective for meeting the mission and goals of the ESD.

The Board recognizes that the district is connected to a statewide electronic communications system (the K-20 Network) which provides Internet access and interactive video conferencing. This network allows opportunities for students, staff, and the educational community to communicate, learn, access, and share information. The ESD dedicates the property comprising the network and grants access to it by users only for the educational activities authorized under this policy and administrative regulations and under the specific limitations contained therein.

The Board directs the superintendent to provide training and procedures that encourage the widest possible access to electronic communications systems by staff, students, and the educational community while establishing reasonable controls for the lawful, efficient, and appropriate use and management of the system.

R334.1 The following administrative regulations apply to the use of e-mail, Internet services, voice mail, video conferencing, use of the statewide K-20 electronic communications network, file servers, printers, user work stations and other electronic media by ESD 112 employees and students.

R334.2 Use of Electronic Communications Systems

ESD electronic communications systems are provided for business and educational purposes only. All use of the system must be in support of education and research and consistent with the mission of the ESD. Employees and students will use electronic communications systems in a responsible, ethical, and informed manner.

R334.2a ESD does recognize that some personal mail will traverse its mail network; such correspondence should be kept to a minimum.

R334.2b Any use of the Internet and computer systems must be in conformity to state and federal law, network provider policies and licenses, and ESD policy. Contact the Human Resources Department for copies of referenced materials.

R334.2c Employees and students with Internet access may download only software with direct business or educational use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.

R334.2d Employees and students will respect the rights, property, and confidentiality of others and will not access, copy, rename, alter, delete or transmit the files, data or information of others without permission or a valid reason related to the user's employment with the ESD.

R334.2e Subscriptions to mailing lists, bulletin boards, chat groups, commercial on-line services, and/or other information services must be pre-approved by the Division administrator.

R334.2f Diligent effort must be made to conserve system resources; for example, users should frequently delete e-mail and unused files.

R334.3 Unacceptable and/or Illegal Uses of Communications Systems

The following actions are strictly prohibited by ESD and may lead to disciplinary action:

- 1) Use of the system for solicitation for private or personal commercial purposes, the solicitation and/or distribution of non-ESD related materials; particularly matters of a personal nature for personal gain (use of the system for charitable purposes must be approved in advance by the superintendent or designee).
- 2) Attempting to gain unauthorized access to the ESD's communications systems or going beyond a person's authorized access. This includes attempting to log in through another person's account or password, accessing another person's file, or misrepresenting other users on the system.
- 3) Deliberate attempts to disrupt or modify the operation of the communications systems, to destroy data by any means, and/or compromising the confidentiality of the ESD's records.
- 4) Use of inappropriate language that is obscene or profane. Displaying or transmitting sexually explicit images or messages.
- 5) Use of communications systems to harass another person. Harassment is persistently acting in a manner that distresses or annoys another person and is unwelcome by that person.
- 6) Use of the system to access, store, or distribute obscene or pornographic material.
- 7) Knowingly or recklessly communicating false, fraudulent, or defamatory information about a person or the agency.
- 8) Re-posting messages that were sent privately, without the permission of the person who sent the message.
- 9) Lobbying, endorsing, or promoting affiliation with a particular political party or person, or ballot measures.
- 10) Originating or forwarding chain letters.
- 11) The unauthorized installation, use, storage, or distribution of copyrighted software or materials on ESD computers.

12) Encryption of communications so as to avoid security review.

R334.3a Users need to remember that they are always identifiable as having an account at ESD 112 (user@esd112.org). When expressing personal views, users should always make it clear whether they are representing themselves or the ESD.

R334.4 No Expectation of Privacy

ESD 112 in no way guarantees the privacy of electronic communications. Employees and students should not consider their Internet usage, e-mail communication, or voice mail to be private or confidential.

R334.4a All electronic mail, conferencing data, and voice mail stored on ESD equipment is considered ESD property. The ESD reserves the right for any reason to access and disclose all messages and electronic data sent over its electronic mail system or stored in its files.

R334.4b Authorized ESD employees may periodically check usage at any time and without notice.

R334.4c The ESD has the right to delete or retain any or all electronic files, including e-mail, of current ESD employees and of employees who are no longer employed by the ESD.

R334.4d Employees should be aware that their electronic communications files may be discoverable in litigation and subject to disclosure under the state public records laws.

R334.5 Internet Access/Passwords

User IDs and passwords help maintain individual accountability for Internet usage. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account.

R334.5a No person shall have access to the Internet system without having received appropriate training and an account name.

R334.5b A signed Individual User Release Form must be on file with the ESD. Students under the age of 18 must have the approval of a parent or guardian.

R334.5c Under no circumstances should a user provide his or her user ID or password to another person with the following exception: Supervisors shall require all employees to provide their communication systems passwords to a designated individual for the purposes of authorized access to the systems.

R334.5d Users should change passwords regularly and avoid easily guessed passwords.

R334.5e All accounts inactive or unused for three months or more will be removed.

R334.6 Personal Security

- R334.6a Personal information such as complete names, addresses, and telephone numbers and identifiable photos should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher and parent or guardian. All users should not disclose, use, or disseminate personal identification information regarding minors without authorization.
- R334.6b Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.
- R334.6c Students should notify their teacher or other adult, and staff should notify their supervisors, whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications.
- R334.7 Filtering and Monitoring
- R334.7a Filtering software or services must be installed and used on all computers with access to the Internet, which will block or filter access to visual depictions that are obscene, child pornography, or harmful to minors. When adults are using the Internet, materials which are obscene and child pornography must still be filtered or blocked.
- R334.7b Educational staff will, to the best of their ability, monitor minors' use of the Internet provided by the ESD, and will take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web, and restrict their access to materials harmful to minors.
- R334.8 ESD Web Sites
- The ESD will establish a Web site and will develop Web pages that will present official information about the ESD and its affiliates.
- R334.8a The superintendent will designate a Director of Web Publishing who is responsible for developing and maintaining the ESD Web site.
- R334.8a1 A Web publishing team will develop style and content guidelines for official ESD materials and develop procedures for the placement and removal of such material.
- R334.8a2 All official material posted on the ESD Web site must be approved by the Director of Web Publishing.
- R334.8b Web publishing procedures will be maintained in the ESD 112 Administrative and Operational Guidelines Manual.
- R334.9 Cooperation with Law Enforcement Authorities
- The ESD will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities through the ESD communications systems.

R334.10

Inappropriate/illegal use of ESD communication may result in cancellation of that employee's privileges to use some or all forms of communications systems and may result in further discipline up to and including termination of employment. Modification or loss of access privileges, and/or civil or criminal action under state or federal law may also result from violations of this policy.