

## Denver Public Schools

### Policy EGAEB – Internet Policy



Denver Public Schools provides a wide-area network service that connects district facilities to each other and to the Internet at large. Access to the Internet offers vast and unique resources to both students and teachers. The district's goal in providing this service is to promote educational opportunities to schools by facilitating resource sharing, innovation, and communication. The Internet is an electronic network of government agencies and regional and state networks. The smooth operation of a network that provides both in-district and worldwide access depends upon the proper conduct of each end-user.

Users must adhere to the guidelines of this policy in order to acquire and maintain network access. Violation of any of the provisions of this policy may result in:

- termination of access
- denial of future access
- possible disciplinary action.

#### Definitions:

1. **Illegal activities** – include, but are not limited to, any activities in violation of local, state, and/or federal laws.
2. **Obscene activities** – include activities in violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle. This includes retrieval of or access to any sexual explicit materials.
3. **Inappropriate use** – includes any activities conducted in violation of this policy or additional activities deemed inappropriate by system administrators.
4. **System administrators** – employees of the school district whose job functions include oversight of the district's computer network.
5. **Dangerous information** – information that if acted upon could cause damage, present a danger, or cause a disruption to the district or the community-at-large.
6. **Compromising personal safety** – revealing personal contact information relating to themselves or other persons.

The district provides filtering to restrict access to obscene, pornographic, or other material that is harmful to minors. The district does not guarantee that such material will never be encountered. On a global network it is impossible to control all materials, and even casual users may easily discover or come across controversial material. The school district believes that the valuable information and interaction available on this worldwide network far outweighs that possibility that users may access material that is not consistent with the educational goals of the district.

The use of the district's network is a privilege, not a right, and must be treated as such by all users. In appropriate use may result in a cancellation of this privilege. The following activities are expressly prohibited:

1. Using the district's network for any or in support of any illegal or obscene activity, and/or inappropriate use.
2. Using the district's network for any inappropriate non-district-related business and/or commercial purpose, product advertising, or support of any political or lobbying activity.
3. Vandalizing the network or network resources, which includes, but is not limited to, any malicious attempt to harm, destroy, or alter data on the district's network, including introduction of any computer virus.
4. Attempting to access restricted data or to disrupt the use of the network for other users.
5. Using profanities or language that is generally offensive, defamatory, harassing, or threatening to another individual and/or group.
6. Creating or accessing dangerous information.
7. Violating copyrights or interference with license agreements. This includes, but is not limited to, software, unaccredited use of text, graphics, photographs, electronic data, or interference with the privacy rights of individuals or entities without their authorization. Plagiarizing any information gathered via the district's network is also prohibited. Users have no proprietary ownership in materials placed on the district's network, unless such material is otherwise covers by copyright.
8. Providing access to the district's network to unauthorized users.
9. Sharing electronic mail account passwords, leaving passwords available in obvious locations, or leaving "signed on" computers unattended.
10. Compromising personal safety.
11. Allowing minors to access inappropriate matter on the Internet.
12. Disclosure, sale, and dissemination of personal information regarding minors.

Communication conducted over the district's network is not private and district staff may, in conducting network supervision and maintenance, review and inspect directories or messages. The district reserves the right and will access stored records with or without reasonable cause to assure compliance with this policy.

The school district makes no warranties that the functions of its network system will meet any specific requirements. Nor will the district be responsible for any damages suffered through use of the network. This includes loss of data, non-deliveries, miss-deliveries, or service interruptions. Use of any information obtained through the district's network is at each user's risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through the Internet.