

INSTRUCTIONAL SERVICES

Regulation 6531

Library, Media and Technology Services

Acceptable Use of the Internet

The following guidelines regulate District network and Internet usage:

Responsibilities

1. District network and Internet access is a privilege, not a right.
2. The Board directs that staff will integrate thoughtful use of Internet information resources throughout the curriculum.
3. Student access to telecommunications and networked information resources shall follow guidelines developed for the selection of appropriate instructional materials and shall be directed to resources evaluated prior to use whenever possible.
4. Since access could extend beyond previewed resources, the staff will supervise and provide developmentally appropriate guidance and instruction to students in the appropriate and effective use of such resources.
5. Students are responsible for good behavior and appropriate language on school computer networks, just as in classrooms and other areas of the school.
6. The educational value of student Internet access is the joint responsibility of students, parents, and employees of the District.
7. Students and staff will respect and protect password/account code security, as well as restricted databases files, and information banks.

Rights and Privileges

District network and Internet access is provided for students and staff to pursue educationally-related communication, research and other activities. Access to Internet services will be provided to students who agree to act in a considerate and responsible manner.

1. Students will submit a properly signed Acceptable Use Agreement, which includes staff and parental/guardian permission, to the principal or designated building network administrator.

2. Before accessing District Internet services, each employee will submit a properly signed Acceptable Use Agreement to the principal or designated building network administrator.
3. A network account will include a District assigned user name and password, assuring that access is the responsibility of the student or staff. In some cases the Network administrator may issue a limited "class" account to groups of students which may be used for specific purposes for a specific amount of time. **These passwords/account codes shall not be shared with others; nor shall students or staff use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal law.**
4. Access to electronic mail (E-mail) is a privilege and designed to assist students and staff in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes.

Restrictions

The following activities are not permitted on District electronic resources:

1. Accessing, uploading, downloading, transmitting, displaying, or distributing obscene, abusive or sexually explicit language or material or descriptions of destructive devices or **otherwise objectional material under current District Board policy or legal definitions.**
2. Damaging or **stealing** computer hardware or software, computer systems or computer networks; vandalizing, damaging or disabling databases or networks through intentional mis- or overuse of electronic distribution, **placement of unlawful information**, or the spreading of computer "viruses" through the inappropriate use of files or diskettes. **Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet.**
3. Violating copyright, or otherwise using another person's intellectual property without his or her prior approval or proper citation; entry into restricted information on systems or network files, creating or maintaining archival copies of downloaded Internet materials unless the source indicates that the materials are in the public domain. Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their education or employment.

4. Using the network for personal gain, commercial purposes, or to engage in political activity, or any activity which is not classroom or workplace related.
5. Sharing passwords/account codes with others; using another party's password except in the authorized maintenance and monitoring of the network; trespassing in another person's folders, work or files, **violation of another person's right to privacy.**
6. Participating in chain letters, "chat rooms" or Multiple User Dimensions (MUDs), with the exception of those bulletin boards or groups that are created by teachers for specific instructional purposes or employees for specific work related communication.
7. Engaging in activities commonly described as "hacking", including, but not limited to, unauthorized review, duplication, dissemination, removal, damage, alteration or theft of files, passwords, computer systems, or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.
8. Using inappropriate language, including vulgarities or obscenities, or other inappropriate references; libeling others.
9. Violating local, state or federal statute.
10. System users may not reveal addresses or telephone numbers or photographs of students, employees, or other individuals during E-mail transmissions.
11. The District E-mail system is designed solely for educational and work related purposes. E-mail files are subject to review by District and school personnel.

Security

The District shall use filtering, blocking or other technology to protect students and staff from accessing Internet sites that contain any form of communication that is obscene, pornographic or harmful in nature. the District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA) **and the Neighborhood Internet Protection Act. (NICPA).**

Disclaimers

1. The District makes no warranties of any kind, either expressed or implied, for the access to the Internet being provided.

2. The staff, school and District are not responsible for any damages incurred, including, but not limited to loss of data resulting from delays, **non-delivery** or interruption of service, for the loss of data stored on District resources or for personal property used to access District resources.
3. The District will not be responsible for the accuracy, nature, or quality of information stored on District resources or gathered through District-provided access. **The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.**
4. The District will use technical or manual means to regulate Internet access and information, however, these methods do not provide a foolproof means for enforcing the provisions of this Regulation.

Consequences

The consequences for violating the District's Acceptable use of the Internet Policy include, but are not limited to, one or more of the following:

1. Parent Conference
2. **Removal of restricted files and/or** suspension of District Network privileges;
3. Revocation of Network privileges;
4. Suspension of Internet access;
5. Revocation of Internet access;
6. Suspension of computer access;
7. Revocation of computer access;
8. In-school suspension;
9. Out-of-school suspension;

10. Expulsion; or
11. Employee disciplinary action up to and including dismissal;
12. Referral to law enforcement officials

02/26/03

Revised:
Revised: February 7, 2002
Approved: July 22, 1999
Adopted: March 5, 1998
University City School Board

03-137um