

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees exclusively for instructional and administrative purposes and in accordance with administrative regulations.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with District policies. [See DH, FNC, FFI, FO and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements, consistent with the purposes and mission of the District and with law and policy governing copyright. [See EFE]

INTERNET SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Guide students to access appropriate materials, as well as block materials that are harmful to minors;
2. Provide student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities; and
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

FILTERING

The District shall use filtering devices or software that blocks Internet access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may

disable the filtering device for bona fide research or other lawful purpose.

MONITORED USE

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use for educational or administrative purposes.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet.

The Superintendent or designee shall oversee the District's electronic communications system.

The District's system shall be used only for administrative and educational purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District shall provide training to employees in proper use of the system and shall provide all users with copies of acceptable use guidelines. All training in the use of the District's system shall emphasize the ethical use of this resource.

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individuals the owner specifically authorizes may upload copyrighted material to the system.

SYSTEM ACCESS

Access to the District's electronic communications system shall be governed as follows:

1. With the approval of the immediate supervisor, District employees shall be granted access to the District's system.
2. The District shall require that all passwords be changed every 90 days.
3. Students completing required coursework on the system shall have first priority for use of District equipment after school hours.
4. Any system user identified as a security risk or having violated District and/or campus computer-use guidelines may be denied access to the District's system.

CAMPUS-LEVEL
COORDINATOR
RESPONSIBILITIES

As the campus-level coordinator for the electronic communications system, the principal or designee shall:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system at the campus level.
2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements shall be maintained on file in the principal's office.
3. Ensure that the employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
5. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
6. Set limits for disk utilization on the system, as needed.
7. Ensure that all campus Web sites are hosted on District servers.
8. Ensure that all campus domain name registration and maintenance is completed through a central account.

INDIVIDUAL USER
RESPONSIBILITIES

Employees shall use District-issued technology rather than personal technology for business purposes. District technology support personnel shall not load software, provide wireless access, assign passwords, or provide technical support so that employees can use personal technology devices for business use. Any exception to this, such as cellular phones, shall comply with approved District procedures.

The following standards shall apply to all users of the District's electronic information/communications systems:

ONLINE CONDUCT

1. The individual in whose name a system account is issued shall be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
4. System users must purge electronic mail in accordance with established retention guidelines.
5. System users may redistribute copyrighted programs or data only with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
6. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may noncommercially redistribute a public domain program. System users shall be responsible for determining whether a program is in the public domain.
7. District employees shall be considered public servants. The online presence of employees shall not be in conflict with District policies and the District's acceptable use guidelines of technology equipment.

VANDALISM
PROHIBITED

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance shall be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above shall result in the cancellation of system use privileges and shall require restitution for costs associated with system restoration, hardware, or software costs.

FORGERY
PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

CONSENT
REQUIREMENT

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner, or individual the owner specifically authorizes, may upload copyrighted material to the system.

Original work created by District students shall require written permission from the student (and the student's parent if the student is a minor) to be posted on a District Web site or to be transmitted via any District television or radio transmission. Classroom assignments shall be exempted from this requirement, but teachers shall approve classroom assignments for appropriateness and acceptability before posting or transmitting.

No personally identifiable information about a District student shall be posted on a Web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy. [See CQ(EXHIBIT) and policy FL]

Original work created by employees may be displayed on the District Web site or transmitted via District television or radio. The District shall consider that submission provides permission to post these employee items. If the work is not created in the scope of the employee's job responsibility, and if it includes a copyright notice on the material, the employee must give permission before posting or transmission.

INFORMATION
CONTENT / THIRD-
PARTY SUPPLIED
INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student knowingly bringing prohibited materials into the school's electronic environment may be subject to a suspension and/or a revocation of privileges on the District's system and shall be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment shall be subject to disciplinary action in accordance with District policies.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Typing messages in capital letters are the computer equivalent of shouting and are considered rude, be polite.
2. Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited, use appropriate language.

3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Revealing personal addresses or phone numbers of the user or others is prohibited.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

TERMINATION /
REVOCAION OF
SYSTEM USER
ACCOUNT

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's account or of a student's access shall be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District shall not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District shall not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District shall cooperate fully with local, state, or federal officials in any investigation concerning or relating to the misuse of the District's electronic communications system.

INTELLECTUAL
PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.