

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

AVAILABILITY
OF ACCESS

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

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.

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.

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 allow monitoring of their use and to comply with such regulations and guidelines. (See CQ Exhibit) Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with Irving Independent School District policies. [See DH, FN series FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the Irving Independent School District.

INTERNET SAFETY

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

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use and dissemination of personally identifiable information regarding students.
5. Educate students about Internet safety, cyberbullying awareness and response and about appropriate online behavior, including but not limited to interacting with other

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

individuals on social networking Web sites online gaming and in chat rooms.

FILTERING

Each District computer with Internet access shall have a filtering device or software that blocks 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 private. Designated District staff shall be authorized to monitor such communication at any time to ensure appropriate use

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.

SECURITY BREACH
NOTIFICATION

Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected person or entities in accordance with the time frames established by law.

The District shall give notice by using one or more of the following methods:

1. Written notice
2. Electronic mail, if District has electronic mail addresses for the affected persons.
3. Conspicuous posting on the District's Web site.
4. Publication through broadcast media.

Breaches of security involving identity theft shall be in compliance with the District's established Identity Theft Prevention Program enacted on May 4, 2009, as Board Resolution No. 08-09-135. [See Employee

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

DISCLAIMER OF
LIABILITY

Handbook]

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

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

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

The District will provide training to employees in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will 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 will be governed as follows:

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

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

CAMPUS-LEVEL
COORDINATOR
RESPONSIBILITIES

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

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's policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's office.
3. Ensure the employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all campus Web sites will be hosted on District approved servers.
5. 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 mobile devices for district approved programs, shall comply with approved district regulations.

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

ON-LINE 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.
3. System users may not use another person's system account without written permissions from the campus administrator or District coordinator, as appropriate.

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

4. System users must purge electronic mail in accordance with established retention guidelines.
5. System users may upload public domain programs to the system. System users may also download public domain programs redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.
6. Employees shall be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media violates state or federal law or District policy, or interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. (See DH)

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 may 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 will 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 IISD students will require written permission from the student (and the student's parent if the student is a minor) to be posted on a District website or to be transmitted via any District television or radio transmission. Classroom assignments are

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

exempted from this requirement according to TEC Section 26.009, but teachers shall approve classroom assignments for appropriateness and acceptability before posting or transmitting.

No personally identifiable information about a District student will 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 policies at FL]

Original work created by employees may be displayed on the District website or transmitted via District television or radio. The District will 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 an/or objectionable material.

A student knowingly bringing prohibited materials in the school's electronic environment will be subject to a suspension and/or a revocation of privileges of the District's system and will 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 will be subject to disciplinary action in accordance with District policies.

TERMINATION/
REVOCAION OF
SYSTEM USER ACCOUNT

The District shall be authorized to 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 will be effective on the date their principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date is so specified in the notice.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a

DATE ISSUED: 11/15/2010
UPDATE 88
CQ(LOCAL)-X

January 24, 2011

REVISED: October 20, 2008

Page 6 of 7
Exhibit "A" to
Resolution No. 10-11-70
Page 6 of 7

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LOCAL)

particular purpose with respect to any services provided by the system and any information of software contained therein. The District does not warranty that the functions or services performed by, or that the information of software contained therein. The District does not warranty that the functions or services performed by, or that the information of 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 will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.