

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

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

The District's system will be used for administrative and educational purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited. Limited personal use shall be permitted in accordance with District policy.

The District will provide training to employees in the 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.

COPYRIGHT POLICIES

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 an individual who has legally secured authorization from the owner may upload copyrighted material to the system.

INTELLECTUAL PROPERTY RIGHTS

No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or consent from the employee who created the work.

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

CONSENT REQUIREMENTS

No personally identifiable information about a District student will be posted on a Web page under 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.

FILTERING

In accordance with federal and state requirements, the District will employ filtering technology on all computers with Internet Access provided by the District. The Superintendent will direct the Chief Technology Officer, to select, implement, and maintain appropriate technology for filtering Internet sites containing materials considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school. Student filtering will comply with the Federal Child Internet Protection Act (CIPA) at a minimum.

The categories of material considered inappropriate and to which access will be blocked will include, but are not limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g. bomb making); and on-line gambling.

REQUESTS TO DISABLE FILTER

A review committee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The committee will make a recommendation to the Chief Technology Officer regarding approval or disapproval of disabling the filter for the requested use.

SYSTEM ACCESS

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

1. Students in grades K – 12 will be granted access to the District's system-by the system administrator, as appropriate.
Secondary students will be assigned an individual account or password.
2. As appropriate and with written approval of the immediate supervisor, District employees will be granted access to the District's system.
3. The District will require that all passwords be changed as appropriate.
4. Any system user identified as a security risk or who has violated District and/or campus computer-use guidelines may be denied access to the District's system.
5. All users will be required to sign a user agreement annually for issuance or renewal of an account.
6. Students who are completing required course work will have the highest priority access to the system and District equipment.
7. Elementary teachers may apply for a class account and in doing so will be ultimately responsible for use of the account.

CHIEF TECHNOLOGY OFFICER RESPONSIBILITIES

The Chief Technology Officer for the District's electronic communications system or campus designee will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for use of the District's system.
2. Ensure that all users of the District's system annually complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's office or supervisor's office.
3. Ensure that employees supervising students who use the District's system will provide training on the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent.
7. 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.
8. Be authorized to set limits for data storage within the District's system, as needed.

9. Be authorized to establish procedures regarding the creation, retention and storage of electronic mail.

INDIVIDUAL USER RESPONSIBILITIES

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

ONLINE CONDUCT

1. Individuals issued a system account will be responsible for its proper use at all times.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communication system.
4. System users may not encrypt communications in order to avoid security review by system administrators. Use of proxy servers, web proxies, or other similar technologies is also prohibited.
5. System users may not use another person's user account without written permission from the campus administrator or District coordinator.
6. System users must delete electronic mail in accordance with established retention guidelines.
7. System users must observe copyright law, district policy and regulations. They may not redistribute copyrighted programs or data unless permission to do so is stated in the program documentation or is obtained directly from the copyright holder.
8. System users must avoid actions that may introduce viruses to the system. Examples of such actions are: opening e-mail messages from unknown senders and loading data from unprotected computers.
9. System users may not upload any programs to the system without prior approval for the Software Review Committee. System users may not download software for their own use or redistribute a District provided program.
10. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
11. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
12. System users of district electronic mail must exercise care so that recipients or readers of mail messages do not assume the messages represent the position of the District or school, whether or not that was the user's intention.
13. System users may not waste District's communications system resources.
14. System users may not gain or attempt to gain unauthorized access to resources or information.
15. System users may not attach or install any equipment to the District's system without prior approval from the Chief Technology Officer or his representative.

16. System users may employ removable media if needed to support educational activities. Users must insure that all such devices pose no hazard to the District's system and that their use does not violate the Acceptable Use Policy.

Student users must adhere to the standards listed above and to the following:

17. Students may not distribute personal information about themselves or others through the electronic communications system. Personal information includes, but is not limited to, personal addresses and telephone numbers.
18. Students must exercise caution in on-line activities. They should not make appointments to meet people whom they meet on-line and should report to a teacher or administrator if they receive any request for such a meeting.

SYSTEM RESOURCES

All users will be assigned a fixed amount of storage for electronic mail and data. Users will be required to routinely review and purge unwanted or unneeded files and messages. In cases where additional storage is needed to meet assigned responsibilities, the Chief Technology Officer will allot additional capacity as appropriate.

Under these guidelines, users will be allocated the following storage capacity:

- 500 megabytes for electronic mail storage
- 1 gigabyte for data storage

All electronic mail messages older than 30 days in the Outlook Delete and Sent Folders will be permanently deleted automatically.

Bandwidth utilization is monitored. System users who routinely monopolize excessive amounts of bandwidth will be notified and their usage will be examined. Permission to use large amounts of bandwidth will be granted on a case by case basis by the Chief Technology Officer.

VANDALISM PROHIBITED

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

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

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, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION CONTENT / THIRD PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that, despite the District's use of lawfully mandated technology protection measures, 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 who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

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

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

PARTICIPATION IN CHAT ROOMS, NEWSGROUPS AND SOCIAL NETWORKS

Students are prohibited from participating in any chat room, newsgroup, or social group accessed on the Internet unless such participation has been assigned and is supervised by a teacher as part of a classroom assignment. Such participation is permissible for employees, in accordance with District policies. Circumventing the district internet filter for the purpose of gaining access to social networking or other blocked communication sites will result in immediate disciplinary action.

COMMUNICATION TOOLS

Students may utilize electronic communication tools only for an educational purpose and only under the direct supervision of a teacher. Examples of such communication tools are: Video Broadcasting, Pod Casting, Blogs, Instant Messaging, Videoconferencing, Such participation is permissible for employees, in accordance with District policies.

DISTRICT WEB SITE

The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be submitted to the District Webmaster. The District Chief Technology Officer will establish guidelines for the development and format of Web pages controlled by the District.

No commercial advertising will be permitted on a Web site controlled by the District.

SCHOOL OR CLASS WEB PAGES

School or class web pages must be approved by the campus principal, conform to the policies that govern the campus newspapers and be controlled by an AISD staff member. The campus principal will designate the staff member responsible for managing the campus's Web page. Teachers will be responsible for compliance with District rules in maintaining their class web pages. Pages which contain damaging or derogatory information or which present the district in a negative manner will be removed. Persons responsible for creating or posting such content may be subject to disciplinary action.

Any links from a school or class web page to sites outside the District's computer system must receive approval from the campus principal.

No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's account or of a student's access for violation of District policies or regulations will be effective on the date the principal or Chief Technology Officer 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 does 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 does 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, 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.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Do not pretend to be someone else when sending/receiving messages. This is considered inappropriate.
4. Do not transmit obscene messages or pictures.
5. Be considerate when sending attachments by e-mail. Large files may be rejected by the recipient's system or may be in a format unreadable by the recipient.
6. Do not disrupt the use of the network by other. Using the network to do so is prohibited.
7. Limit storage on the network to professional or educational materials.
8. Routinely delete emails in Outlook and unneeded files in My Documents.