



EMPLOYEE ACCEPTABLE USE GUIDELINES

General Guidelines for Employees

The following information is provided so that students, parents and staff are aware of responsibilities involved in the efficient, ethical and legal use of technology resources. Anyone using a District device will be required to adhere to all District policies and to Internet Safety and Acceptable Use Guidelines in order to be granted access to District technology resources. 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 administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and compliance with such regulations and guidelines. Access to the District electronic communications systems, including the Internet, shall be made available to students and employees for instructional and administrative purposes and in accordance with administrative regulations. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Electronic mail transmissions and other use of the electronic communications system are not private and may be monitored at any time by designated District staff to ensure appropriate use.

Consent Requirements

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

Filtering

The superintendent will appoint a committee, to be chaired by the executive director of technology, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers and mobile devices provided by the school. The categories of material considered inappropriate and to which access will be blocked will include, but not be 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 online gambling.

Request to Access a Blocked Site

The committee or designee will consider requests from users who wish to use a blocked site for bona fide research, instruction, or other lawful purposes.

System Access

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

1. Students in all grades will be granted access to the District's system as appropriate. Students may be assigned individual accounts.
2. As appropriate and with the approval of the immediate supervisor, District employees will be granted access to the District's system.
3. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.
4. Any system user identified as a security risk or as having 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.

Executive Director of Technology Responsibilities

The executive director of technology will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system complete and sign annually 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 or supervisor's office.
3. Ensure that employees supervising students who use the District's system provide training emphasizing 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 other 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. Set limits for data storage within the District's system, as needed.

Individual User Responsibilities

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

1. The individual in whose name a system account is issued will 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 or guidelines.
3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. System users may not use another person's system account without written permission from the campus or district administrator as appropriate.
6. Students may not distribute personal information about themselves or others by means of the electronic communications system unless instructed to do so by an administrator, counselor, librarian or teacher for instructional purposes. This includes, but is not limited to, personal addresses and telephone numbers.
7. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any request for such a meeting.
8. System users may not use the network for financial or commercial gain, advertising or political lobbying.
9. System users must purge electronic mail in accordance with established retention guidelines.
10. System users may not redistribute copyrighted programs or data except 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.
11. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages/attachments from unknown/unexpected senders and loading data from unprotected computers.
12. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
13. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
14. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
15. System users may not waste District resources related to the electronic communications system.
16. System users may not gain unauthorized access to resources or information.

17. Employees who identify or know about a security problem are expected to convey the details to an administrator.

Vandalism

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are 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 technology protection measures as required by law, 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 knowingly bringing 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 knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

District Website

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 directed to the designated Webmaster. The District Webmaster will establish guidelines for the development and format of Web pages controlled by the District. No personally identifiable information regarding a student will be published on a Website controlled by the District without written permission from the student's parent. No commercial advertising will be permitted on a Website controlled by the District.

School or Class Webpages

Schools or classes may publish and link to the District's site Web pages that present information about the school or class activities, subject to approval from the Webmaster. The campus principal will designate the staff member responsible for managing the campus's Web page under the supervision of the District's Webmaster. Teachers will be responsible for compliance with District guidelines in maintaining their class Web pages. Any links from a school or class Web page to sites outside the District's computer system must receive approval from the District Webmaster.

Extracurricular Organization Webpages

With the approval of the District Webmaster, extracurricular organizations may establish Web pages linked to a campus or District Web site; however, all material presented on the Web page must relate specifically to organization activities and include only student-produced material. The sponsor of the organization will be responsible for compliance with District guidelines for maintaining the Web page. Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District." Any links from the Web page of an extracurricular organization to sites outside the District's computer system must receive approval from the District Webmaster.

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. Pretending to be someone else when sending/receiving messages is prohibited.
4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Termination of User Account

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

Blocking Internet Content

When a teacher needs a specific web resource for a valid instructional purpose, but the content is blocked by the CISD filter, the teacher should work with the Helpdesk to submit a help ticket. If students or teachers encounter content that is inappropriate, a help ticket should be submitted to identify the resource to personnel in the Helpdesk.

Employee Signature: _____

Date: _____

Printed Name: _____

Employee #: _____

Campus: _____

Department: _____

Job Title: _____