

ELECTRONIC COMMUNICATION & DATA MANAGEMENT ACCEPTABLE USE POLICY

District resources have been invested in computer technology to broaden instruction and to prepare students for an increasingly computerized society. Use of these resources is restricted to students working under a teacher's supervision and to approved purposes only.

Board Intent

It is the intent of the Board to provide access to electronic information resources for District staff, teachers and students. This policy is based on the belief that access to electronic information resources creates critical educational opportunities for students and teachers. The Superintendent or designee shall develop administrative procedures to administer the electronic resources of the District.

The District's system will 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 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.

Consent Requirements

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 owners specifically authorize 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) 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 Education Records Privacy Act and District policy.

System Access and User Responsibilities

Access to the District's Electronic Communications System will be governed as follows:

1. With the written approval of the immediate supervisor, District employees will be granted access to the District's system.
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 gain unauthorized access to resources or information.
4. The District will require that all passwords be changed every 30 days.

5. District employees with accounts will be required to maintain password confidentiality by not sharing the password with students or others.
6. The individual in whose name a system account is issued will be responsible at all times for its proper use.
7. System users may not use another person's system account without written permission from the campus administrator or system administrator, as appropriate.
8. System users may not distribute personal information about themselves or others by means of the electronic communication system.
9. System users must purge electronic mail in accordance with established retention guidelines.
10. Teachers may apply for a class email account and will be responsible for the appropriate use of the account.
11. 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.
12. System users may redistribute copyrighted programs or data only with the written permission of the copyright holder or designees. 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. The "Software Custodian" of the campus/department must be involved in this process.
13. System users may download public domain programs such as free-ware or shareware for their own use on their workstation only. Documentation of the program's free status must also be downloaded and the software must be reported to and documented by the "Software Custodian" of the campus/department. System users are responsible for determining whether a program is in the public domain.
14. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, for financial gain, or illegal.
15. System users may not use an alias or any form of a made up name to access a web site, chat room, or other resource that does not check user ID's. Accesses to those sites are not allowed.
16. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
17. System users may not save or store on District computers materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
18. Students will be granted access to the District's system after appropriate training and with teacher approval as appropriate.
19. Student groups (lab classes) may be granted special log in names that have network rights to shared folders for the storage or transfer of documents and other work necessary for their class. Students will not abuse this right by placing unauthorized material, executables or other items not approved by their teacher.
20. Students and staff members will not use the District's electronic resources and shared network folders and servers for the purpose of "gaming", storing games, or playing games that are not a part of the curriculum for the class they are enrolled in. Students may not bring games on any removable or remote media, including their own computers to play or install using district resources. "Lan parties" using district owned technology equipment, bandwidth, wiring, switches, hubs, etc. is prohibited. The playing of games not purchased and installed on district computers is prohibited.
21. The creation of "shared folders" or "servers" outside of the District's "domain of servers" is prohibited. Lab classes needing servers or network equipment for learning purposes can use that equipment as long as no connection to the Willis ISD WAN or LAN is present. Labs

meeting this definition will be isolated from the Willis ISD WAN or LAN. No workstation on the Willis ISD WAN or LAN can contain more than one network card or more than one network connection. Modems are prohibited in any workstation.

22. Students are not allowed to work on a computer workstation with a teacher or staff member logged into the network.
23. Staff members who have student aides who work in administrative areas, offices, libraries, cafeterias, or other areas where District and Campus administrative programs are accessed are required to have a password protected screen saver to block unauthorized access to their workstation.
24. Students will not be allowed to work in any District or Campus program that is used for administrative, budgetary, accountability, employee and/or student record keeping or processing.
25. Students completing required course work on the system will have first priority for use of District equipment after school hours.
26. Any 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.
27. System users may not waste District resources related to the electronic communications system.
28. The use of all technology equipment and software programs is provided for the conduction of business and in order to help meet the educational objectives of Willis ISD. Personal use of equipment or software, including email and the Internet, is prohibited. All staff members and students are advised that the district archives all email sent and received in Willis ISD for a minimum time period of 7 years. Access to those archived emails is restricted to district administration, law enforcement, court ordered inquires and open records requests as allowed by law.

Director of Technology Responsibilities

The Director of Technology for the District's electronic communications system (or designee) will:

1. Oversee the planning, purchase, operation, maintenance and upgrade of all District electronic communications systems, including but not limited to; email, Internet, data processing, student services, servers, computers and peripherals, telephones, data lines, fiber optic lines, LANs and WANs.
2. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
3. 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 will be maintained on file in the principal or supervisor's office. The inclusion of this AUP in a staff or student handbook with a signature page will satisfy this guideline.
4. Ensure that employees are provided adequate training emphasizing the appropriate use of the District's system and software applications.
5. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed. Unlicensed software may be removed without prior notice.
6. Be authorized to monitor or examine all system activities, files, logon dates and times, user/access logs, and electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
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.
9. Ensure that the District's Internet Access is filtered to avoid exposure to inappropriate materials.

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, possible, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading, sharing 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, hardware or software costs 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 or 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 / Data Ownership

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 will be subject to a suspension and/or a 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 and/or procedures.

All data entered into the data systems or created by an employee during their employment is the property of Willis ISD. Data that is produced in any form and saved to disk(s), hard drives, or network storage areas is the property of Willis ISD. All disk(s) or other storage mediums will be surrendered to Willis ISD upon separation of employment. Willis ISD retains the intellectual and property rights to all data.

Participation in Chat Rooms and Newsgroups

Participation in chat rooms and newsgroups accessed on the Internet is permissible for students, under appropriate supervision and in accordance with educational objectives decided upon by the supervising teacher and with approval of their supervisor. No student will identify himself or herself by full name or address while in a chat room. The supervising teacher must

provide an acceptable name to use in the chat room (i.e. first name only). No student is allowed to enter a chat room that is for anonymous users.

Employees may participate in chat rooms and newsgroups for educational and administrative purposes, as long as the chat room uses traceable email addresses or logons to verify who the actual user is. No access is allowed to anonymous chat rooms where the identity of the end user is not known.

By default, all Internet chat rooms are blocked. Contact the technology office to unblock an appropriate chat room that meets the above requirements.

Internet Access (Filtered)

The District will provide Internet access to all staff and students. Access will be filtered in accordance to applicable rules and laws concerning access of Internet resources by minors. The District will maintain the same standards for adults.

The Technology Director or designee will be the chair of a committee representative of campuses who will review filtering software and pages that are filtered. The committee will decide what categories of pages should be filtered to provide the least restrictive access to the Internet while protecting of students from objectionable materials. Any appeal by an individual to un-block a site will be reviewed by that committee. The committee's decision will be final.

Development of Web Pages

The District has created a World Wide Web server that will provide individuals with Internet accounts access to information about the District and programs. The following guidelines will apply to the posting of pages on the District's web server and are general in nature. A complete and more comprehensive web site guide is also in the technology guidebook for Willis ISD titled "WISD Web Page Guidelines".

1. Students may create web pages with teacher review and approval and in accordance with District and campus guidelines.
2. Student web pages may not be posted on school home pages on the District servers without teacher review for content and linkages and approval by the principal and his/her designee.
3. Pictures cannot be posted on student web pages or on class home pages that allow students to be identified individually by name unless the parent has signed the appropriate form authorizing this posting.
4. Student pages will be published only under the direction of the supervising teacher and after written permission is obtained from a parent or guardian.
5. Teachers may create web pages for publishing to the District's web server using the tools provided by the district. All pages will be in the appropriate template.
6. All pages will be reviewed by the campus webmaster periodically for appropriate content.
7. Each web page subgroup (staff, student, campus subgroups, organizations) can be no longer than 8 pages deep. Campus and administrative groups may have unlimited subgroups and/or organizations as long as they are appropriate and approved by the campus principal or appropriate administrator or director.
8. The District Webmaster or Campus Webmaster, as appropriate, will post web pages to the web server for publishing.
9. Campus Webmasters will be appointed by principals and will be trained in appropriate practices.

10. The District Webmaster will be responsible for the maintaining of the overall Willis ISD web site.
11. All Willis ISD clubs and organizations must publish their "official website" within the Willis ISD website and on the Willis ISD server. School clubs and organizations may not host a site on another outside web server. Booster clubs, PTO organizations and other Willis ISD affiliated groups will be given space on the Willis ISD web server to host their site and must abide by Willis ISD guidelines for their site.

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 or receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Sending electronic messages to all users ("spamming") is prohibited and is reserved for use by the System Administrator. (Send to one distribution group per email if needed for the purposes discussed in this paragraph... no fund raisers or announcements of sales, meetings or other unsolicited flyers are allowed) Email shall not be used to announce school events, programs, fundraisers, or any outside activities, sales or fundraisers. The exception to this is administrative use to disseminate information necessary for the administration and efficient operation of a campus/department.
6. Posting to the electronic bulletin board (announcements/fundraisers, public folder) will be for school-related activities and information only. School calendars are provided in the public folders for this purpose. Contact your campus administration for details on how to get an event posted.
7. A public folder is provided in the email system for employees to post for sale, for rent, garage sale, and other sale or service messages. These types of messages must be posted in this designated area and not emailed to others via email.
8. Revealing or publishing to outside parties the street and/or email addresses or telephone numbers of others is prohibited. The only information published on the web site without an Open Records Act request will be an email list of WISD email addresses or a WISD phone directory.
9. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Termination / Revocation 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 will be effective on the date the principal or System Administrator receives notice of student withdrawal or of revocation of system privileges or on a future date if so specified in the notice.

Failure to follow all guidelines will result in disciplinary action according to District policy and/or the Student Code of Conduct.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed 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 nor 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. Users should be aware that data stored on the system may be lost in a software or hardware failure and should take appropriate steps to backup important data.

Users should be aware that data stored on the system may be lost in a software or hardware failure and should take appropriate steps to backup important data.

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.

Acknowledgment of Receipt and Understanding of these Guidelines:

Your signature in the WISD Employee Manual or the Student Manual, or a parent or guardian's signature indicates your receipt of and your agreement to abide by these guidelines.

Acceptable Use Policy is available for review on-line at Willis ISD Technology Department web page or at the offices of campus administrators or campus computer teachers.