

Acceptable Use Policy of Gilmer Independent School District's Technology Resources

The Gilmer Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the Gilmer schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff. **The use of these technology resources is a privilege, not a right.**

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Gilmer ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Gilmer ISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District Policy.

The Gilmer Independent School District strongly condemns the illegal distribution of software, otherwise known as pirating. Any student/staff caught transferring such files through the Internet/Intranet, and any whose accounts are found to contain such illegal files, shall immediately have their accounts permanently revoked. In addition, all users should be aware that software piracy is a federal offense and is punishable by fine or imprisonment.

Definition of District Technology Resources

The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. **The District reserves the right to monitor all technology resource activity.**

Acceptable Use

The District's technology resources will be used only for learning, teaching and administrative purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District will make training available to all users in the proper use of the system and will make copies of acceptable use guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource.

Software or external data may not be placed on any computer, whether stand-alone or networked to the District's system, without permission from the Superintendent or designee.

Other issues applicable to acceptable use are:

1. Supervision and permission: **Student use of the computers and computer network is only allowed when supervised or granted permission by a staff member.**

2. **Improper use of any computer or the network is prohibited. This includes but not limited to the following:**
 - A. **Users will not load any software and/or programs to Gilmer ISD Computer Systems** without the explicit permission of the Director of Technology.
 - B. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute pornographic, obscene or sexually explicit material.
 - C. Users will not use the school district system to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.
 - D. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that are inappropriate to the educational setting or disruptive to the educational process and will not post information or materials that could cause damage or danger of disruption.
 - E. Users will not connect/use non-district owned computer equipment on the District's system/network without prior approval from the Superintendent or his designee.
 - F. Users will not access or participate in chat rooms, or multi-user environments including but not limited to; MUDs or MOOs; **download or play games**; subscribe to or access listservs; download music files or check, **use non-district services to send or receive email (such as Hotmail, Yahoo, AOL & etc.) unless prior permission** is granted by the Superintendent or his designee.
 - G. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.
 - H. Users will not use the school district system to knowingly or recklessly post false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
 - I. Users will not use the school district system to engage in any illegal act or violate any local, state or federal statute or law.
 - J. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make

deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district system's security, and will not use the school district system in such a way as to disrupt the use of the system by other users.

- K. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.
- L. Users will not use the school district system to post private information about another person or to post personal contact information about themselves or other persons including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, and will not repost a message that was sent to the user privately without permission of the person who sent the message.
- M. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user.
- N. Users will not use the school district system to violate copyright laws, or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software, literary works, music & etc or copying the copyrighted material to or from any school computer, and will not plagiarize works they find on the Internet.
- O. Users will not use the school district system for the conduct of a business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. **Users will not use the school district system to offer or provide goods or services (such as eBay, Bargain & Hagggle, and other online auction sites) or for product advertisement. Users will not use the school district system to purchase goods or services for personal use (such as eBay, Bargain & Hagggle, and other online auction sites) without authorization from the appropriate school district official.**
- P. Users will not use the school district system to access, review, upload, download, store, print, post, or distribute chain letters, solicitations, and like materials. Chain letters of any sort are violations of Federal law, whether or not they ask for money. Chain mail of any sort must not be responded to or forwarded, even if they do not ask for money.

If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. A user may also in certain rare instances access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate district official.

Limited Expectation of Privacy

1. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.
2. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.
3. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy.
4. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. **Parents have the right to request the termination of their child's individual account at any time.**
5. School district employees should be aware that data and other materials in files maintained on the school district system/computers may be subject to review, disclosure or discovery under the Texas Penal Code, Computer Crimes, Chapter 33.
6. **The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities and activities not in compliance with school district policies conducted through the school district system.**

System Access

Access to the District's network systems will be governed as follows:

1. Students will have access to the District's resources for class assignments and research with their teacher's permission and/or supervision.
2. Teachers with accounts will be required to maintain password confidentiality by not sharing the password with students or others.
3. With the approval of the immediate supervisor, district employees will be granted access to the District's system.
4. **Any system user identified as a security risk or having violated District Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.**

Campus Level Coordinator Responsibilities

As the campus level coordinator for the network systems, the principal or designee will:

1. Be responsible for disseminating and enforcing the District Acceptable Use Guidelines for the District's system at the campus level.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

Individual User Responsibilities

The following standards will apply to all users of the District's computer network 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 guidelines.

3. System users may not use another person's system account without written permission from the campus coordinator or principal, as appropriate.
4. System users are asked to purge electronic mail or outdated files on a regular basis.
5. System users are responsible for making sure they do not violate any copyright laws.
6. The most important prerequisite for someone to receive a District System account is that he or she **take full responsibility for his or her own actions.**

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or material, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. **Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district guidelines and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33.** This 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, possible prosecution, and will require restitution for costs associated with system restoration, hardware, or software costs.

Forgery Prohibited

Forgery or attempted forgery of electronic 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.

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 outside the District's networks that may contain inaccurate and/or objectionable material.

A student 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.

Network Etiquette

System users are expected to observe the following network etiquette (also known as netiquette):

1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
2. Pretending to be someone else when sending/receiving messages is prohibited.
3. Transmitting obscene messages or pictures is prohibited.
4. Revealing such personal information as addresses or phone numbers of users or others is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

6. Users must be sensitive to the public nature of shared facilities and must not print or display on screens in such locations images, sounds or messages which are likely to create an atmosphere of discomfort or harassment for others.
7. Be polite. For example, messages typed in capital letters are the computer equivalent of shouting and are considered rude.

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 campus coordinator receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Consequences of improper use

Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

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 fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

The District uses a variety of vendor supplied hardware and software. Therefore, 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 user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor 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 necessarily 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 computer systems and networks.