

Policies and Procedure

INTERNET TERMS AND
CONDITIONS OF USE FOR
STAFF

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. In a global network it is impossible to control all materials and an industrious user may discover controversial information. The Grand Prairie Independent School District firmly believes that the valuable information and interaction available on this world-wide network far out weighs the possibility that users may procure material that is not consistent with the educational goals of the District.

These guidelines are provided here so users are aware of the responsibilities. In general this requires efficient, ethical and legal utilization of the network resources. If a Grand Prairie Independent School District user violates any of these provisions, his or her access will be terminated and future access could possibly be denied.

Proper behavior, as it relates to the use of district technology resources, is no different than proper behavior in all other aspects of Grand Prairie 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 CQ (Local).

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 use of the network must be in support of education and research and be consistent with the educational objectives of the Grand Prairie Independent School District. Use of other organization's network or computing resources must comply with the rules appropriate for that network.

Transmission (that is, uploading or downloading) of any material in violation of any national or state regulation is prohibited. This includes, but is not limited to:

- Copyrighted material
- Abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, illegal material
- Material protected by trade secret
- Commercial activities such as conducting private business on the Internet
- Further transmission for advertisement or political use is forbidden.

SECURITY

The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. School Personnel will deem what is inappropriate use and their decision is final. The administration, faculty, staff, and parents may request to deny, revoke, or suspend specific user privileges.

PARENTAL ACCESS

The parents or legal guardian have the right to access or examine materials held in the student's electronic folder.

WARRANTY

The Grand Prairie Independent School district makes no warranties of any kind, whether expressed or implied, for the service it is providing. Grand Prairie Independent School District will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the district's negligence or user errors or omissions. Use of any information obtained via the Internet is at your own risk. Grand Prairie Independent School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

SECURITY

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the network, you are required to notify a system administrator or school personnel. Do not demonstrate the problem to other users. Do not use another individual's account. Someone identified as a security risk or having a history of problems with other computer systems may cause the user to be denied access to Internet.

VANDALISM

Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to access, harm, alter, or destroy data of another user, Internet, or any of the above listed agencies or other networks that are connected to any of the Internet backbones. This includes, but is not limited to, the uploading or creation of computer viruses.

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.

TERMINATION/
REVOCATION OF SYSTEM
USER ACCESS

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

Violation of GPISD's policies and procedures concerning, the use of computers and networks will result in the same disciplinary actions that would result from similar violations in other areas of GPISD.

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. 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.

These policies are subject to modification from time to time.

NETWORK ETIQUETTE

Users are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- a) Be polite. Do not send abusive messages.
- b) Use appropriate language. Do not swear; use vulgarities, sexually suggestive language, or any other inappropriate language. Illegal activities are strictly forbidden.
- c) Do not reveal your personal address or phone number or the address or phone number of other students or colleagues.
- d) Note that electronic mail (E-mail) is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities.
- e) Do not use the network in such a way that you would disrupt the use of the network by other users.

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. 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.
4. Students may not distribute personal information about themselves or others by means of the electronic communication system.

DISTRICT LEVEL
COORDINATOR
RESPONSIBILITIES

The technology coordinator for the District's electronic communications system 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 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 proper use of the system.
6. Be authorized to establish a retention schedule for messages on technology systems and to remove messages posted locally that are deemed to be inappropriate.
7. Set limits for data storage within the District's system, as needed.

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 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. Copies of District Policies EFE, EFE (Local), EFE(E) are available at all sites and on-line.
6. Electronic mail can be purged from the system with notice to if needed in order to conserve network resources.
7. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
8. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

9. 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.
10. System users may not gain unauthorized access to resources or information.

ELECTRONIC MAIL AND
ADDITIONAL
TECHNOLOGY GUIDELINES

Email has become one of the most used communications tools in both offices and classrooms. The following points are important to keep in mind:

- The software and hardware that provides us email capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication. Although we do not have staff members who actively monitor email communications, the contents of any communication of this type would be governed by the Open Records Act. WE would have to abide and cooperate with any legal request for access to email contents by the proper authorities.
- Users will be issued only one district email account.
- Since email access is provided as a normal operating tool for any employee who requires it to perform their job, individual staff email addresses must be shared with interested parents and community members who request to communicate with staff in this fashion.
- Requests for personal information on students or staff members should not be honored via email. It is critical for a personal contact to be made with any individual requesting personal information. This relates particularly to any requests for student grades, discipline, attendance or related information. In addition, security information such as username or password should not be sent via email for any reason.
- It is an expectation that email be checked at least once a day. Staff should be expected to return email communications to parents or other public members who have legitimate business request within 24 hours whenever possible. Request from outside agencies for information do not fit into this same category and can be handled with a different timeline or in a manner consistent with previous experience in working with similar requests.

- Incoming email that is mis-addressed will remain "undeliverable". We do not have the staff available to personally inspect all messages of this type and forward them to the proper person. Please be certain that you give out your correct email address.
- Since email access is primarily provided for school business related use, please do not forward messages that have no educational or professional value. An example would be any number of messages that show a cute text pattern or follow a "chain letter" concept. These messages should be deleted and the sender notified that messages of that nature are not appropriate to receive on your district email account.
- Please use the "groups" function of our email system appropriately. Do not sent messages to an entire staff when only a small group of people actually needs to receive the message. In accordance with established procedures, using email for commercial enterprises is prohibited.
- Attachments to email messages should include only data files. AT no time should program files (typically labeled ".exe") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they're "launched" or started. If you receive an attachment like this or any questionable attachment, please delete the email message immediately without saving or looking at the attachment.
- Students will not be issued individual email accounts. For any projects that involve email communications, use either your district account as a facilitator to the activity, or, work with a Technology Staff member to activate a special project account for a limited item.

ADDITIONAL GUIDELINES

- On occasion, we need to reformat hard drives. Reformatting completely erases all contents of the hard drive. All district software such as Microsoft Office, which is consistent throughout the district, will be reinstalled. All other approved software, purchased by the building, will need to be reinstalled by the campus. We will not reinstall unapproved copies of software nor will we be able to retrieve any personal data files.

With this in mind, please keep any installation disks of specific school purchased software in an identified location at your campus should the need for reinstallation arise. The user is personally responsible for making backups of any data files that you store on your local hard drive.

- All computer and video hardware should be shut down each evening. This includes CPU's, monitors, printers, TVs and VCRs. The exception to this would be laser printers. They can be left on since they include automatic power-saving features.

PURCHASING OF STAND-
ALONE COMPUTER
SOFTWARE (Non-Networked
Software

Purchasing of "Stand-Alone" computer software **should be originated by the campus or department** needing the software. If the purchase does not exceed \$500.00, the software may be purchased from any reputable vendor. However, the purchasing department recommends that all software purchases be made from vendors on the "Approved Vendor List" whenever possible. It is also good practice to ask multiple vendors to quote on the software needed to insure a competitive environment among vendors. Asking multiple vendors to quote on software needed will almost always result in better pricing.

If the purchase exceeds \$500.00 but not more than \$2,000.00, the software should be purchased from a vendor on the "Approved Vendor List".

If the purchase is greater than \$2,000.00 but less than \$10,000, written quotations from at least three (3) approved vendors must be received and documented.

If the purchase exceeds \$10,000.00, please contact the purchasing department for assistance.

The "Approved Vendor List" can be viewed from the following WEB site:

<http://www.gpisd.org/gpisd/administration/finance/vendorlistcat.pdf>

In addition, the state of Texas offers a list of approved vendors that can be viewed from the following WEB site: <http://www.gsc.state.tx.us/ecat/index.html> The use of these vendors is considered appropriate by the purchasing department.

Another source for legal acquisition of computer software is through the Department of Information Resources. This information can be viewed from the following WEB site: http://www.dir.state.tx.us/busops/dir_store/software.htm
Acquisition of software through the DIR is considered appropriate by the purchasing department.

SOLE SOURCE

Contact the purchasing department before purchasing any software under a Sole Source justification.

PURCHASING OF
NETWORKED COMPUTER
SOFTWARE(Software than Runs
in a shared fashion on the network)

Please work with the Technology Department to insure that the software will work on the GPISD network before writing any purchase order.

After approval from the Technology Department, follow the same procedure as "Stand Alone" software purchases.

CONTACT: EXECUTIVE DIRECTOR
OF TECHNOLOGY

7/10/97

8/14/01
Revised

10 of 10