
Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

Dear Grossmont District Employee,

The Information Age brings with it a host of educational opportunities and potential problems. It is important that you understand your rights and privileges when using Grossmont Union High School District resources in this environment. This document describes the computer, telephone, information, and network resources made available by the District and your responsibilities and obligations in the use of these resources. All District employees are required to read and sign this document.

An electronic version of this document is available at <http://intranet.guhsd.net/documents/empaup.pdf>.

Thank you for your time and cooperation.

Rick Roberts – Executive Director, Information and Technology Services

The GUHSD Computer and Network Environment

The District has created extensive networks with information, telephone and computing resources for staff and student use. These resources are provided to allow you and others in the District to perform your tasks effectively in meeting the goals and needs for which the District was established.

By nature, design, and function, the District's computer network and resources must provide a relatively "open" environment. While automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources, the primary responsibility for maintaining the security of this information and its resources lies with you, the employee.

Improper use of any of these resources can cause problems related to the needs of some or all employees and students in the District. Violation of specific local, State, and Federal laws referenced later in this document may call for prosecution under the law including fines and imprisonment. The District may take disciplinary action against employees for misuse of computer, network, and information resources.

Privacy of District Records – Student, Staff, and Business Information

Both student and employee records are protected by various State and Federal laws –

State Statutes:

- Education Code, section 67100
- Information Practices Act of 1977 (Civil Code section 1798)
- Public Records Act (Gov. Code section 6250)
- Penal Codes, Section 502

Federal Statutes:

- Federal Family Educational Rights and Privacy Act of 1974
- Federal Privacy Act of 1974
- Electronic Communications Privacy Act of 1986

During your employment with the District, you will have access to either student or employee and business information that is confidential. It is your responsibility to safeguard this information from unauthorized persons. You shall not seek to use personal or confidential information for your own use or personal gain. You must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, magnetic tape, email, network storage, etc.), paper, photograph, and microfiche information. Included under this precaution is the disposal of any privacy related materials.

Ownership

It must be understood that the District's business information, telephone, network, computer and software resources, peripherals and supplies are District property, provided to meet District needs. They do not belong to individuals, but are only "loaned" for the purposes required for your position while you are employed by the District.

Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

This specifically means that you MAY NOT use your computer, its software, peripherals or supplies for personal, commercial, or non-District purposes. For example, you may not use your District computer to store or maintain your personal business. Use of your workstation and its software, printers, faxes, copiers, and other peripherals for personal work may be permitted where approved by your supervisor in advance and when it is done outside your normal work hours.

Use of Telephones, Cell Phones, and Voicemail

Telephones and cell phones are provided to conduct the business of the District. In many cases, voice mail is also provided. These services are intended to provide a means of communication for employees to contact parents and students, agencies, vendors, other institutions and government officials. When using these services, your comporment should be businesslike and professional. Private use of the phones should be kept to a minimum. Employees are responsible for any charges incurred when using District phones or cell phones for purposes not directly related to their job duties or assisting in emergencies. Cell phones should never be used while operating a vehicle. Employees with assigned cell phones are expected to take appropriate precautions to prevent damage to unit, including theft, exposure to moisture and extreme temperatures.

Use of District Laptop Computers

Laptop computers may be issued to regular faculty members teaching three or more sections. They are provided for the purpose of preparing/delivering lessons and keeping classroom records. With the convenience of portability comes an increased risk of theft, loss, or damage. Teachers are expected to take all reasonable precautions to keep laptops issued to them safe and secure. When transporting laptops off campus, please take care to not leave them in unattended automobiles, hot or damp places, or where there is an increased risk of damage or theft. Teachers are to follow established District checkout procedures for taking their laptop home overnight, on weekends, and over holidays and breaks. Teachers who choose to take their laptop home must have homeowner's/renter's insurance covering damage or loss of the equipment. District insurance is in force while the machine is on campus. Misuse, abuse, neglect, willful damage, termination of employment, or violation of district policy while using a laptop shall be grounds for the District to request the laptop's return.

Use of Personally Owned Software or Equipment

The District attempts to ensure that all hardware and software meet specific standards which will operate without causing disruption of the District's computer and network resources. Therefore, the use of personally owned software or software that can be downloaded from the Internet as well as personally-owned computer hardware, is not permitted except where authorized by the Assistant Superintendent of Educational Services or his designee.

Software Copyright Law

Violations of copyright law have the potential of costing the District millions of dollars. You are prohibited from installing any software without having proof of licensing. You may not install software licensed for one workstation on multiple machines. You should be aware that if, for example, you purchase a new workstation, you must also purchase new software licenses for the software that will be installed on it. If the computer being replaced will be retired from use, the software may be removed from it and transferred to a new workstation.

Use of the Internet and Intranet

The Internet provides an extremely valuable resource for learning and communicating with people throughout the world. It can be a marvelous tool to enhance student and staff education and productivity. Unfortunately, the Internet also contains a large amount of information that is inappropriate for use in an educational institution.

While it is hoped that employees will enjoy the use of Internet resources, it must be emphasized that these resources are provided at District expense to enhance your job function and maximize your job effectiveness. Employees are not to let personal use of the Internet encroach on or displace time spent performing their work duties. Personal use of the Internet should be restricted to breaks or lunch periods, or before or after work hours. Inasmuch as every transaction you complete on the Internet represents to the world our District and everything it stands for., it is imperative that employees not use the Internet in such a way as to bring civil or criminal liability or public reproach upon the District.

Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

Materials obtained from the Internet are copyrighted and, with proper citation, limited educational use is permitted under the Principle of Fair use as contained in U.S. copyright law. These materials may not be redistributed on the Internet or in any other manner without written consent of the copyright owner or as prohibited by law. Materials are protected by copyright whether they bear copyright information or not.

The District Intranet is distinct from the Internet. It consists of those networked electronic resources within the Grossmont Union High School District. Access to many of these resources is public, thus contributing to the Internet at large. Others are accessible only from within the District network or by password. Note that access to District-only resources, such as subscription electronic research portals is not to be shared with others outside the District. Access to the student information system, though accomplished through a web browser is to be guarded as you would guard access to your bank account. Never leave a session in the student system without logging out and closing the browser window, no matter how brief the interruption.

No one may attach to the District network any wireless device without prior approval of the Director of Technical Services, Business Services. This includes, but is not limited to: wireless computers, PDAs, wireless hubs or base stations.

Use of Computer Resources

The computing resources of the District are used by thousands of students and employees. In order to ensure that these resources are available and working properly, your personal use of these resources must not negatively impact others.

For example, you may not attempt to break into computer systems or their resources to which you have not been granted authorization. You may not attempt to maliciously alter, erase, damage, destroy or make otherwise unusable or inaccessible any data, software, computer, or network system. Attempts or actions of this nature are a felony and may result in any combination of disciplinary action and/or prosecution and fines including litigation costs and payment of damages under applicable local, State, and Federal statutes.

Use of Network Storage

In addition to network file servers used in a classroom setting, the District provides each employee with 1 gigabyte of network storage called an eBackpack. This space is accessible from anywhere on the Internet and includes public and private layers of access. Private drop-boxes are for students to turn in assignments electronically without seeing each other's work. Public folders are for disseminating course materials, announcements, and instructional web pages. Employees are to observe all applicable laws (including copyright) and District policies in the use of eBackpacks. Storage and account access may not be shared or used for any purpose other than the direct support of instruction or job performance.

Your Computer Account

In order for you to utilize the District's computer and network resources, you will be assigned a "user id" and password. Based on your position and your supervisor's authorization, you may be provided with access levels which allow you to view, create, alter, delete, print, and transmit information.

You are responsible for maintaining the security of your personal account and may not release it for use by any other individual. You must accord your user account the same significance as your hand-written signature. Failure to do so by releasing this information to another individual may be considered false representation and result in disciplinary action.

This means that it is extremely important that you use a password that cannot be guessed by others through knowledge about you. For example, never use personal names such as children or pets or names that begin or end with numbers. Never use your Social Security Number, bank PIN or words which can be found in any dictionary, names spelled backwards, or adjacent keys on a computer keyboard (i.e., QWERTY). All of the above provide an easy way for a "cracker" to break into a computer system and, using your rights and privileges, cause damage and destruction. You must also never write down your user id or password unless you store it in your personal possession or other location away from your place of work. Even then, you should write it in such a way that no clue is given as to the purpose for its use. Please contact the Information & Technology Services if you suspect someone else may have accessed your account. It is a simple matter to change your password in a few seconds, but may take days to reconstruct damaged

Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

records or computer systems if someone breaks in with your account rights! Where you have the ability to change your own password, make a habit of periodically changing passwords for these accounts.

You should never leave your workstation unattended while signed on to any account; doing so allows anyone to sit at your workstation and, using your rights and privileges, perform destructive acts. This has been the most common method used in the past for students to make changes to their own or others' records.

Under certain circumstances, user id's and passwords may be shared by a group of employees where doing so makes information access convenient with a minimum of administrative overhead. Examples include District-subscribed online services that teachers may wish to access from outside of the District network. Group id's and passwords should be held in confidence and never shared with students. If you suspect that the security of such information has been compromised, notify the network administrator at once.

Only employees may have direct publishing (write privilege) access to District web, mail, and list servers. Those who assume responsibility for posting student work must never delegate this responsibility to students or colleagues. Do not store passwords where students may have access to them. Periodically change your password.

Computer Viruses

Despite the development of new technologies to combat malicious viruses, worms, and other damaging programs that attack computers and networks, these problems persist. The District attempts to maintain anti-virus software in order to minimize the impact of these viruses, but it is your responsibility to take precautions to protect your computer and all others throughout the District.

For example, avoid opening email attachments from people you do not know. If someone you do know sends you an attachment, contact them and verify what the purpose of the attachment is. Ask them if they are sure no viruses may have invaded their attachment.

Likewise, do not download any software from the Internet unless directed to and authorized by the District Office. It is not unknown for even a very respectable company to unknowingly release products which include hidden or unknown viruses. Do not share any downloaded software with others until you have verified that it does not harbor viruses.

Electronic Mail

The District encourages the use of electronic mail (email) to enhance communication and business activities. The following policies are necessary to ensure appropriate use and to prevent or limit disruptions to work activity and computer services. Please read carefully:

Cautions About The Use Of Electronic Mail

The nature of electronic mail at this date makes it susceptible to misuse. Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both within the District as well as externally throughout the world.

In addition, while email accounts may be password protected, it is up to the individual user to ensure that a password is set and that the password is one that cannot be easily guessed or "hacked".

Because of backup procedures in force with the District's computer services, the fact that you have "deleted" an email message does not necessarily mean that it cannot be retrieved.

Users of the District's email services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All email sent or received by individuals through District employee accounts is the property of the District and may be requested by your supervisor and examined **with just cause**.

Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

There is no guarantee that email received was in fact sent by the purported sender, since it is a simple matter, although a violation of this policy, to disguise the sender's identity. Furthermore, email that is forwarded may be modified by the forwarder. As with any document, if you receive a message which appears unusual or which you feel may be questionable, check with the purported sender to verify authorship and authenticity.

While the District does not have the time nor inclination to monitor or read individual email messages, in the event that questionable or inappropriate use is suspected or known, such email may be examined and may be cause for disciplinary action ranging from revoking your email account up to termination. Users should also be aware that in the general course of business, System Administrators and email operators may require observation of messages in order to verify system operation.

SPAM

The District maintains a system for limiting the amount of unwanted or offensive email received from the Internet. Known as SPAM, much of this email is automatically generated by computer programs and is often used to propagate computer viruses, or distribute pornography and fraudulent business offerings. The email may appear to have come from a trusted address and others may receive such messages that falsely appear to have come from you. The District's email filtering system cannot eliminate all SPAM and it is possible that benign messages may occasionally be blocked. Please check your daily Spam Quarantine Summary to forward misidentified mail or to whitelist the sender. You may also fine-tune your own personal spam tolerance settings.

Email – Personal Use

Private or personal non-commercial use of the District's email is permitted as long as it is not excessive and does not interfere with the District's normal business practices and the performance of the individual's tasks. Individuals should exercise sound judgment and sensitivity to others when exchanging personal messages in the workplace.

Email – State, Federal, And Copyright Laws

In addition to this policy, use of the District's email services is subject to all applicable Federal and State communications and privacy laws as well. In particular, users need to be aware that attaching programs, sound, video, and images to email messages may violate copyright laws, and data files containing employee and/or student information is subject to all privacy laws.

Email Restrictions

Electronic mail may **not** be used for:

- Unlawful activities
- Commercial purposes
- Personal financial gain
- Use that violates this policy or other State and Federal policies
- Any form of harassment
- Chain letters, sending or forwarding
- Spam mail, that is, to exploit listservers or other broadcast systems which amplify widespread distribution of unsolicited email
- File storage. (Use eBackpack.)
- Mail bombs, that is, to re-send the same email repeatedly to one or more recipients with the intent to interfere with the recipient's use of email
- Any other use which interferes with computing facilities and services of the District or its employees
- Personal fund-raising

Email and Representation

Users shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the District unless they are appropriately authorized, explicitly or implicitly, to do so. Where appropriate and based on context, an appropriate disclaimer would be, "These are my own statements and views and do not represent those of the Grossmont Union High School District."

Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

Email – False Identity

Employees shall not employ a false identity in sending email or alter forwarded mail out of the context of its original meaning.

Email – Misuse Of Computing Services

Email services shall not be used for purposes that could reasonably be expected to cause, either directly or indirectly, excessive strain on District computing facilities, or cause interference with others' use of email, email systems, or any computing facilities or services. For example, attaching large files over 1 megabyte and sending these to multiple users or repeatedly to the same user is a violation of this policy. The District's email system is not designed for file storage. Such use is prohibited. Please use your eBackpack for storing or archiving files.

Email – Security And Confidentiality

The confidentiality of electronic mail cannot be assured. Users should exercise extreme caution in using email to communicate confidential or sensitive material.

Email – Virus Dangers

As mentioned, proper precautions must be taken to guard against the infection of computers and files by viruses. Likewise, using email attachments to distribute viruses and/or worms and other damaging software is common-place today. You should never open email or attachments unless you are expecting them. Even if someone you know well sends you an attachment, ask them before you open it if they are using the latest anti-virus software. If they aren't certain or don't know, contact the Technical Services department and we will arrange to install District-licensed anti-virus software.

Email – Archiving And Retention

The District maintains an ongoing backup schedule of computer data in order to ensure that these facilities may be restored to use in the event of damage and/or destruction. Because of this practice, email may be stored on backup media for extended lengths of time. Messages which a user assumes to be deleted may be able to be restored if demanded by the appropriate District authority.

Each user should consider whether they want to archive their personal messages to their workstation's hard drive or other disk media on some sort of regular basis, as there is always the possibility that information may be lost due to software or hardware problems. The District has policies in place for the length of time email is retained on-line. After 14 days current email may be moved into the user's "trash" where it may still be recoverable for a short time. Thus, users should be careful not to consider email as a long-term filing system.

While the District maintains a backup of all email, it is not feasible nor our practice to restore lost or damaged email.

Email – Classroom Use by Students

Teachers who permit students to use email accounts other than those hosted by the District shall emphasize that the District has no control over such accounts. Nevertheless, teachers shall require students to report any and all suspicious or threatening email received.

Other Services

Please note that this policy addresses issues common to all teachers and employees. Other specific policies may apply to those working in specialized environments or completing specialized tasks such as advising students involved in web publishing. If you have any questions about this or other policies, please do not hesitate to ask the Director of Educational and Library Technology or the Director of Systems Integration.

Grossmont Union High School District

Employee Computer, Telephone and Network Acceptable Use Policy

Employee Acknowledgment the Rules of this Policy

I acknowledge receipt of the Grossmont Union High School District Employee Computer, Telephone and Network Acceptable Use Policy (updated 6/13/07).

I acknowledge that I have read and understand the Acceptable Use Policy.

(Please **PRINT**) First Name – Middle Initial – Last Name

Signature

Date

School/Location

Position