COMPUTER, TELEPHONE AND NETWORK ACCEPTABLE USE

BOARD POLICY

Computer and Network Environment

The District has created extensive networks with information, telephone and computing resources for employee and student use. In addition, the District provides a large and continuously growing number of computer workstations, printers, peripherals, software, training and supplies to all sites. These items are provided to allow employees to perform tasks effectively in meeting the goals and needs of the District.

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 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

It is probable that during employment with the District, employees will have access to either student or employee and business information that is confidential. It is the responsibility of employees to safeguard confidential information from unauthorized persons. Employees shall not seek to use personal or confidential information for their own use or personal gain. Employees 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, etc.), paper, photograph, and microfiche information. Included under this precaution is the disposal of any privacy related materials.

COMPUTER, TELEPHONE AND NETWORK ACCEPTABLE USE

BOARD POLICY

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 their position while you are employed by the District.

Use of Telephones, Cell Phones, and Voicemail

Telephones and/or 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, employees should always reflect a businesslike and professional demeanor. Private use of the phones should be kept to a minimum.

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 Superintendent or his designee for IT services.

Software Copyright Law

Violations of copyright law have the potential of exposing the District substantial risk of liability for damages. Employees are prohibited from installing any software without having proof of licensing. Employees may not install software licensed for one workstation on multiple machines. Employees should be aware that if, for example, a school purchases a new workstation, the program 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

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 job function and maximize 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. In as much as every transaction completed 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.

Materials obtained from the Internet may be copyrighted. However, with proper citation, limited educational use may be 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.

Use of Computer Resources

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

For example, no one may attempt to access computer systems or their resources unless proper authorization has been granted. No one may 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 may constitute 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.

Your Computer Account

In order to utilize the District's computer and network resources, employees will be assigned "user IDs" and passwords. Based on an employee's position and his or her supervisor's authorization, the employee may be provided with access levels which allow him or her to view, create, alter, delete, print, and transmit information.

Employees are responsible for maintaining the security of their personal account and may not release it for use by any other individual. Employees must accord a user account the same significance as a 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 employees use a password that cannot be guessed by others through knowledge about the employee. For example, employees should never use personal names such as children or pets or names that begin or end with numbers. Never use Social Security Numbers, bank PINs 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 hacker to break into a computer system and, using employee rights and privileges, cause damage and destruction. Employees must also never write down user IDs or passwords unless stored in the employee's personal possession or other location away from the place of work. Even then, the ID or password should be written in such a way that no clue is given as to the purpose for its use. Employees should contact the IT coordinator if they suspect someone else may have accessed their account. It is a simple matter to change a password in a few seconds, but may take days to reconstruct damaged records or computer systems if someone breaks in with employee account rights! Where an employee has the ability to change his or her own password, the employee should make a habit of periodically changing passwords for these accounts.

Employees should never leave their workstation unattended while signed on to any account; doing so allows anyone to sit at an employee's workstation and, using the employee's 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 IDs 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 IDs and passwords should be held in confidence and never shared with students. If an employee suspects that the security of such information has been compromised, the employee should 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. Passwords may not be stored where students may have access to them. Passwords should be periodically changed.

Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, and other damaging programs that attack computer and network resources. The District attempts to maintain anti-virus software in order to minimize impact of these viruses, but it is your responsibility to take precautions to protect your computer and all others throughout the District.

Employees should be very aware of opening email attachments. When in doubt, they should NOT be opened.

Likewise, employees should not download any software from the Internet unless directed to and authorized by the Superintendent or IT designee. It is not unknown for even a very respectable company to unknowingly release products which include hidden or unknown viruses. Employees should not share any downloaded software with others until they have verified that it does not harbor viruses.

COMPUTER, TELEPHONE AND NETWORK ACCEPTABLE USE

BOARD POLICY

Electronic Mail

The District encourages the use of electronic mail (email) to enhance communication and business activities. Users of this service need to be aware however that this technology is still developing, and policies like this one are necessary to ensure appropriate use and to prevent or limit disruptions to work activity and computer services.

- **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 caus**e.

  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 encryption of email is a potential solution to ensure authenticity, it is an emerging technology that is not in widespread use and rather difficult to use consistently. Technology will mature such that it becomes practical and easy to use in the near future.

  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.

- **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
  - Spam mail or mail "bombs"
  - Use that violates District, state or federal policies
  - Any other use which interferes with computing facilities and services of the District

- **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 Gold Oak Union School District."

- **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 one (1) megabyte and sending these to multiple users or repeatedly to the same user is a violation of this policy.

COMPUTER, TELEPHONE AND NETWORK ACCEPTABLE USE

BOARD POLICY

- **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 commonplace today.

- **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. This schedule is fourteen (14) days for current email, after which it is placed 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.

COMPUTER, TELEPHONE AND NETWORK ACCEPTABLE USE

BOARD POLICY

PERSONNEL

Employee Use of Technology

The Gold Oak Union School District Superintendent recognizes that technology can enhance employee performance by improving access to and exchange of information, improve the quality of instruction, and facilitate operations. All employees are expected to learn to use the available electronic resources that will assist them in their jobs. As needed, staff will receive training in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use the electronic resources of the District only for purposes related to their employment. Such use is a privilege that may be revoked at any time.

Employees should be aware that computer files and communications over electronic networks, including e-mail and voice mail, are not private. This technology should not be used to transmit confidential information. To ensure proper use of technology, the Superintendent or designee may monitor the technological resources at any time, without notice or consent.