Trinidad School District #1 File: EHA

# General Computer and Information Systems Procedures

## Purpose:

In support of its mission of teaching and community service, the TRINIDAD SCHOOL DISTRICT #1 provides access to computing and information resources for students, faculty, and staff within institutional priorities and financial capabilities. The Computer Use Procedure contains the governing philosophy for regulating faculty, student, and staff use of the System's computing resources. It spells out the general principles regarding appropriate use of equipment, software, networks and data. In addition to this policy all members of the TRINIDAD SCHOOL DISTRICT #1 community are also bound by local, state, and federal laws relating to copyrights, security, and other statutes regarding electronic media

The rules and conditions in the following document apply to all users of all systems in all locations TRINIDAD SCHOOL DISTRICT #1. Willful violations of the following policies may result in disciplinary action following normal Human Resources procedures and guidelines in consultation with the appropriate supervisor, which may result in actions up to and including termination and necessary legal action.

## Policy:

In accordance with the Colorado Open Records Act (CRS § 24-72-201 et seq.), it should be recognized that all public records are open for inspection by any person at reasonable times. The basic definition of "public records" in CORA is "all writings made, maintained, or kept by the state . . . ." This includes information and e-mail on state employees' computers. The only public records that fall outside this policy are records identified in specific exceptions set forth in CORA, in other Colorado statutes, and in federal law (including FERPA).

The TRINIDAD SCHOOL DISTRICT #1 has the right to monitor any and all aspects of its computer and telecommunications systems including employee e-mail, voice mail, and file structures on any TRINIDAD SCHOOL DISTRICT #1 system. TRINIDAD SCHOOL DISTRICT #1's right to monitor its computer system and telecommunications equipment includes, but is not limited to, monitoring sites users visit on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users, and reviewing e-mail sent and received by users. The computer and telecommunication systems are provided to the employees to assist them in meeting the requirements for the performance of their positions in TRINIDAD SCHOOL DISTRICT #1. Employees should not have an expectation of privacy in anything that they create, send, or receive on TRINIDAD SCHOOL DISTRICT #1 systems. Since systems are provided for TRINIDAD SCHOOL DISTRICT #1 business, all transactions and all data on the systems are considered to be business-related and therefore owned by the TRINIDAD SCHOOL DISTRICT #1. All systems owned by TRINIDAD SCHOOL DISTRICT #1 are to be used for TRINIDAD SCHOOL DISTRICT #1 business purposes only. TRINIDAD SCHOOL DISTRICT #1's control of all information on TRINIDAD SCHOOL DISTRICT #1 computers does not implicate intellectual property rights. Intellectual property rights are governed by Federal statutes.

Systems users should adhere to the following rules which apply to all computer and telecommunications resources including file servers, desktops, notebooks, laptops, handheld devices, network infrastructure, PBXs, voice mail systems, Internet connectivity, bulletin board systems, e-mail systems and other resources.

This policy will be updated from time to time at TRINIDAD SCHOOL DISTRICT #1's discretion. For example, changes to this policy will be made periodically by TRINIDAD SCHOOL DISTRICT #1:

(a) When there is a change in applicable state or federal law;

(b) When new technology becomes available that increases TRINIDAD SCHOOL DISTRICT #1's exposure to risks and consequently requires new control procedures.

.

**Purchasing**

All technology related purchases including: servers, desktop computers, laptop computers, notebooks, PDAs, monitors, projectors, external storage devices, printers, scanners, network infrastructure hardware, keyboards, mice, software and any/all peripherals MUST 1st be approved by the appropriate supervisor, and 2nd be approved by the Superintendent, or as delegated to the Director of Technology. Any purchases made not following these criteria will not be supported by the IT Department and will not be attached to any technology equipment belonging to TRINIDAD SCHOOL DISTRICT #1. Donated equipment is not required to meet these criteria. Any equipment purchased prior to the date of acceptance or revision of this policy, will be supported by the IT Department.

**Computer Lab Addition or Expansion**

Any addition of new computer labs must be presented to the IT Department. Where in the IT Department will determine the feasibility of the labs' location, in relation to LAN accessibility, electrical needs, and time table required to complete the project. The IT Department will also address the issue of cost in relationship to purchasing new LAN hardware, LAN wiring, installation of LAN wiring, computers, printers, peripherals, and any other technology related items requested/required for the use of the lab.

**User IDs and Passwords**

All employees accessing any TRINIDAD SCHOOL DISTRICT #1 computer or communication system must have a unique User ID and Password. This includes user accounts for the Local Area Network, Servers. To maintain system security, users are not to login as another user. Generic logins will not be issued unless an application requires it with no work-around.

To protect themselves and the confidentiality of data, users are prohibited from disclosing their passwords to others. Logins and passwords are not to be written down and/or displayed or kept in places such as desk drawers, keyboard trays, etc. If a user suspects that their password has been disclosed, they are required to change it immediately. User accounts are not transferable to temporary employees; if someone will be filling in for a user during an absence, a temporary account must be used for the interim employee. Security will be set up to make the user's data accessible by the person filling in.

### Unattended Computers

To protect themselves and the confidentiality of data, users are required to logout, shut down their workstations, or activate a Windows screen saver with password protection when leaving their computers unattended, even if leaving for only a few minutes.

### Logging Off / Shutting Down

Users are to completely log off and turn off their computers by selecting "Shutdown Computer" when leaving for the day. Users should always stay until their system shuts down according to the normal shutdown process. If the computer fails to shut down properly, the districts IT Department should be notified. Never turn off the power before the shutdown process is completed to avoid possible file corruption

### Software

All users must comply with all software licenses, copyrights, and all other state and federal laws governing software licensing and intellectual property.

The installation, removal or copying of any software including customized programs, in-house developed applications, off the shelf software, gaming programs, public domain software (also known as shareware or freeware), or screen savers is prohibited by any user other than IT staff. Personal backgrounds or wall paper may be used subject to supervisor approval.

Exceptions are as follows:

, In areas where computer instruction is taught provisions will be made for the installation of software as part of normal classroom activities.

, Compiling any application as part of a classroom activity does not constitute the installation of software. .

, The District shall ensure areas are set up so that faculty and staff may review and demo software that may meet their needs.

, Exceptions can be made on a case by case basis to allow individuals power user permissions for operation of their computer system.

## Internet and E-mail

Users may be granted access to the Internet for informational and business purposes.

The use of any TRINIDAD SCHOOL DISTRICT #1 resources for electronic mail is made available for District business, including academic pursuits. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the District. Any such incidental and occasional use of District electronic mail resources for personal purposes is subject to the provisions of this policy.

All non-business usage, such as outside course/school or charitable work, would need to be authorized by the individual's supervisor.

Users are not allowed to download software from the Internet (including browser Plug-ins). If you require software to be downloaded that is on the Internet, please submit a request to the District's IT Department for assistance.

Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or other unlawful material may not be sent via e-mail, viewed and downloaded, or passed by any other form of communication or be displayed or stored. Exceptions may be made for various instructional purposes.

Creation and forwarding of non-business e-mail including advertisements, chain mail, solicitations, promotions, political material, etc., are not allowed.

## Hardware

TRINIDAD SCHOOL DISTRICT #1-owned computer equipment and peripherals may not be removed from the premises, relocated, or loaned to others without prior written authorization from Technology Department or appropriately authorized individual. Some employees who travel frequently may be assigned a laptop or portable device by the district. Computers or peripherals not owned by TRINIDAD SCHOOL DISTRICT #1 may be used on the District premises only as a stand-alone device not connected to any TRINIDAD SCHOOL DISTRICT #1 computer, network or telecommunication system. Exceptions to this may be the connection of personal computers to projection systems or other devices that are not part of the production network. This must be supervised by a District employee. TRINIDAD SCHOOL DISTRICT #1 is not liable for any damages to personal systems used in this manner. Only Authorized IT Staff are allowed to install applications or configure these devices. Some employees may be allowed to connect either their own computers or District owned computers to TRINIDAD SCHOOL DISTRICT #1 network from home or when traveling on District business, using a secure TRINIDAD SCHOOL DISTRICT #1-assigned VPN software. However, Technology Department personnel are not allowed to service any computer not owned by TRINIDAD
SCHOOL DISTRICT #1

## Personal Usage of Software/Hardware

TRINIDAD SCHOOL DISTRICT #1-owned computer equipment and software applications may not be used for personal business at any time or for any reason, outside of incidental use.

Any software not owned by TRINIDAD SCHOOL DISTRICT #1 may not be installed on TRINIDAD SCHOOL DISTRICT #1-owned computer equipment. All computer equipment assigned to employees must be returned intact upon termination of employment.

## Backups

The Technology Department is responsible for performing nightly backups on network and servers only. Local PC hard drives will not be backed up in any way. For this reason, the use of local PC hard drives for file storage is greatly discouraged. All users are required to log out of the system completely at the end of every work day. If a user has not properly logged out of the network at the time of backup, active files cannot be backed up.

Local PC hard drives will be erased when employment ends or the PC (Desktop PC, Laptop Computer, PDA, etc.) is taken out of service. Any data on the local PC hard drive is subject to loss and will not be recovered. Any work related documentation would be forwarded to the appropriate individual(s) designated by the supervisor.

## Security Violations

All TRINIDAD SCHOOL DISTRICT #1 employees have a duty to report all information regarding security violations or misuse of hardware or software to either their supervisor and Technology Department immediately in written form.

## Examples of Prohibited Activities

Prohibited activities on TRINIDAD SCHOOL DISTRICT #1 computers and telecommunications systems include but are not limited to:

Sending, receiving, displaying, printing, otherwise disseminating, or storing material that is fraudulent, harassing, illegal, abusive, indecent, embarrassing, profane, sexually explicit, obscene, intimidating, political, or defamatory. Exceptions may be made for legitimate instructional purposes.

Transmitting to others, in any location, images, sounds or messages that might reasonably be considered harassing;

Screen displays of images, sounds or messages that could create an atmosphere of discomfort or harassment for others, especially those considered obscene or sexually explicit;

Attempting to forge electronic mail messages or using someone else’s electronic mail;

Accessing personal interest sites, viewing chat rooms (except chat rooms integrated within the course management system), or using recreational games for other than occasional use.

Using TRINIDAD SCHOOL DISTRICT #1 computers for commercial gain or private profit;

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, music, videotapes, books, or other copyrighted sources, and copyrighted software;

Exporting software or technical information in violation of U.S. export laws;

Posting or e-mailing scams such as “make money fast” schemes or pyramid/chain letters;

Threatening bodily harm or property damage to individuals or groups;

Making fraudulent offers of products, items, or services originating from a user’s account;

Attempting to access the accounts of others, or attempting to penetrate security measures of other entities’ systems (“hacking”), whether or not the intrusion results in corruption or loss of data;

Accessing another person’s computer, computer account, files, or data without permission;

Using any means to decode or otherwise obtain restricted passwords or access control information;

Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain access to any system;

Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., “spamming”, “phishing”, “flooding”, or “bombing”);

Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to data;

Engaging in any other activity that does not comply with the general principles presented above.

## Frequently Asked Questions and Answers

**1. Does the hardware and software purchased by my department from grant funds belong to TRINIDAD SCHOOL DISTRICT #1?**

Yes, it does. The grant funds are almost certainly money provided under a contract between TRINIDAD SCHOOL DISTRICT #1 and the grant source. As such, they are monies of t TRINIDAD SCHOOL DISTRICT #1 and anything purchased or leased or created through the use of that money belongs to the TRINIDAD SCHOOL DISTRICT #1. So this policy applies, and TRINIDAD SCHOOL DISTRICT #1 has the right to access that hardware and software as may be necessary.

**2. Does TRINIDAD SCHOOL DISTRICT #1 have the right to look at my accounts, files, and electronic communications?**

Yes, TRINIDAD SCHOOL DISTRICT #1 officials have a right to look at any user's electronic accounts, files, or communications within the limits established by law. Employees need to understand that there is no absolute right to personal privacy when the employee is using the employer's equipment, including IT resources. TRINIDAD SCHOOL DISTRICT #1 does not routinely monitor the content of files or communications, but may view contents whenever it has a business or legal need to do so.

You should also be aware that the files you maintain on TRINIDAD SCHOOL DISTRICT #1 IT resources may be considered public records and the TRINIDAD SCHOOL DISTRICT #1 may be required to make them available for inspection under the Colorado Open Records Act. In addition, the Act defines $public records$ to include electronic mail messages which means that your email messages also may be subject to public inspection.

**3. Does TRINIDAD SCHOOL DISTRICT #1 have the right to delete my data or block my communications?**

TRINIDAD SCHOOL DISTRICT #1 IT administrators are charged with maintaining and operating the resources for the benefit of all members of TRINIDAD SCHOOL DISTRICT #1. If someone's data consumes so much storage that others are denied storage or if someone's web page attracts so much network traffic that others are denied network access, the administrator of those resources has the right to remove the material. Whenever possible, users are given an opportunity to backup data to other media before it is removed.

**4. Who can work on equipment?**

TRINIDAD SCHOOL DISTRICT #1 faculty, staff and student may use computers. However, only certified IT Staff can service District owned computers, printers, projectors, PDAs, etc. This includes installation of software applications (i.e., Microsoft Word, Excel, Adobe PhotoShop, etc.) TRINIDAD SCHOOL DISTRICT #1 IT Staff will not support computers, PDAs, etc. that do not belong to TRINIDAD SCHOOL DISTRICT #1.

**5. Who installs updates, browsers and plug-ins?**

**Only IT Staff are allowed to install updates, browsers and plug-ins. Some updates, plug-ins, etc. may be installed through a variety of methods that will not require user intervention.**

**6. Who can access my computer ?**

**Your immediate supervisor and the Director of Technology or authorized IT Department personnel. It is recommended that if access to an employees' computer is required, that at least two (2) higher ranking TRINIDAD SCHOOL DISTRICT #1 personnel be present (i.e., accessing an instructor's computer, the building Principal and the Director of Technology; accessing a Principals computer, the Superintendent and the Director of Technology; accessing the Superintendent's computer, the Assistant Superintendent or Acting Superintendent and the Director of Technology.) Please keep in mind as previously stated that information on a TRINIDAD SCHOOL DISTRICT #1 computer is subject to Open Records Act (CRS § 24-72-201 et seq.) A courtesy notification will be made, but will not be required.**

Adopted: December 18, 2008
Effective: January 1, 2009