# FISD Technology Department

# Standard Operating Procedures Manual

# Table of Contents

# I. Mission & Vision

The Fabens Independent School District (FISD) Technology Department works on developing and maintaining a network that provides reliable service to all district staff. Also, we focus on developing a customer service infrastructure that continually seeks to understand and meet customer requirements.

As part of this effort, the following mission and vision statements have been developed:

## Mission

To integrate appropriate technology into the educational environment to promote the use and application of various technological tools needed in modern society for the full development of competence in both students and staff.

## Vision

To be a knowledgeable, customer-focused, empowered, and professional team that continually learns and improves its effectiveness. Provide access to information in its past, present, and future forms with multimedia, multi-sensory methods that are powerful, easy-to-use, and increasingly reduce the constraints of time and space.

# II. Acceptable Use Policy

In the performance of an employee's duties, FISD-provided computer hardware, software, data files, and networks are the property of or are licensed to Fabens Independent School District and are to be used solely for official School Business. All district employees are required to sign an "Acceptable Use Policy". The main points of the AUP are the following:

- Intentional and unauthorized disclosure of personal/confidential information is an invasion of privacy and may result in disciplinary, civil, and/or criminal action.
- It is against district policy to seek out or use district records including, but not limited to, personal/confidential information relating to others for my personal interest or advantage.
- An account and password constitute an employee's signature and that employee is responsible for all entries made under that account. Use of another person's account and password would not absolve someone of responsibility for actions taken under that account and password. Delegation of an account and password for the sole purpose of electronic mail retrieval may be made upon prior approval of one's supervisor.
- Employees must comply with all computer use standards, policies, rules, procedures, and State and Federal laws.

- Failure to comply with this statement may result in disciplinary action, up to and including dismissal.

# III. Password Guidelines

The FISD network is configured so that each staff member using the network is required to have a unique password and user-id. This configuration allows the FISD network to handle a wide variety of complex tasks in a very secure way. However, this security depends upon the users' participation. The following are some security guidelines for staff users of the FISD network.

1. **PASSWORDS CHANGE EVERY 90 DAYS.** While the user-id will always remain the same, the password will have to be changed every 90 days. The system will prompt the user at 90 days and the user will have 6 grace logins to change password. If the password is not changed the user will be locked out and he or she will have to come by the technology department to have the password reset.

2. **CHOOSE A GOOD PASSWORD.** Your password must be a minimum of 5 characters. Must be a unique password and cannot be one of the last (8) eight passwords used. You should select a password that is easy for you to remember, but which is difficult to guess. Do not use your last name, or other simple-to-guess words for your password. Also, do not pick a password just because it is easy to type -- these passwords are also easily guessed. Your password may be a combination of alphabet and numeral characters.

3. **NEVER SHARE YOUR PASSWORD.** Each and every staff user should have his or her, own password do not share your password with your administrator, secretary, or administrative assistants. The user-id can be used to track system activity, only the actual use associated with the password should ever use it.

4. **REQUESTING A PASSWORD OTHER THAN YOUR OWN.** The department/campus administrator must submit a request for someone else's password in writing to the Technology Director.

5. **DO NOT STORE YOUR PASSWORD IN FUNCTION KEYS OR MACROS.** This action seriously degrades the security of the FISD Network. There is a high potential for miss-use of the system when user-id and passwords can be obtained from function key or macro programming.

6. **DO NOT LEAVE YOUR WORKSTATION IN SECURED MODULES.** If you have used your password to get into one of the secured modules (Frontline, Gmail), it is important that you exit back out of that area before leaving your session running unattended.

7. **COMPROMISED PASSWORD.** If an account or password is compromised, report the incident to the Technology Director and your password will be reset.

8. **PASSWORD RESET.** Please contact the technology department.

9. **VIOLATIONS.** Any employee found to have violated this policy may be subject to actions up to and including loss of access to network resources and disciplinary action.

# IV. Email Guidelines

This clarifies the guidelines to electronic mail. Users are reminded that all users of the Fabens ISD's information technology resources, including electronic mail, are subject to all relevant Fabens ISD policies and relevant state and federal laws, including federal copyright law.

Appropriate use of Fabens ISD electronic resources includes instruction, research, service, and the official work of the offices, departments, recognized student and campus organizations, and as described below, incidental personal usage by faculty, staff, and students. Since resources are not unlimited, the district may give priority for resources to certain users or certain groups of users in support of its mission. Consistent with the district's non-discrimination policy, the use of information resources should not be denied or abridged because of race, creed, color, sex, sexual orientation, religion, national origin, age, or physical disability.

**Account Details**
All email accounts will be assigned by the Fabens ISD Technology Department. Email storage unlimited. It is the responsibility of each individual to manage his or her email account this includes archiving, organizing and deleting emails.

**Privacy of Email Files**
Fabens ISD encourages the use of electronic mail and respects the privacy of users. It does not inspect or monitor electronic mail routinely, nor is the district responsible for its contents. Nonetheless, users of electronic mail systems should be aware that, in addition to being subject to authorized access as detailed below, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents.

Users of electronic mail services also should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved on the district systems or any other electronic systems through which the mail has traveled.

Fabens ISD electronic mail services may, subject to the foregoing, be used for ***incidental personal purposes*** provided such use does not interfere with Fabens ISD operation of

information technologies including electronic mail services, burden the Fabens ISD with incremental costs, or interfere with the user's employment or other obligations to the district.
Access by authorized Fabens ISD employees to electronic mail stored on the district's network of computers may be necessary to ensure the orderly administration and functioning of the districts computing systems. Such access, gained for purposes such as to back up or move data, ordinarily should not require the employee gaining access to the electronic mail to read messages. Fabens ISD requires employees, such as system administrators, who as a function of their jobs routinely have access to electronic mail and other electronically stored data to maintain the confidentiality of such information.

Access to electronic mail on the district's network of computers that involves reading electronic mail may occur only where authorized by the Fabens ISD officials designated below and only for the following purposes:

- Troubleshooting hardware and software problems, such as rerouting or disposing of undeliverable mail, if deemed necessary by the Technology Director or his or her authorized designee;
- Preventing or investigating unauthorized access and system misuse, if deemed necessary by the Technology Director;
- Retrieving or reviewing for Fabens ISD purposes Fabens ISD-related information;
- Investigating reports of violation of Fabens ISD policy or local, state, or federal law;
- Investigating reports of employee misconduct;
- Complying with legal requests for information (such as subpoenas and public records requests); and
- Retrieving information in emergency circumstances where there is a threat to health, safety, or Fabens ISD property involved.

In addition to the foregoing, when a Fabens ISD employee leaves employment or when a student graduates or otherwise withdraws from the Fabens ISD, a system administrator may remove the departing employee's or student's email files from Fabens ISD systems in order to conserve space or for other business purposes. An employee's email may be retained and accessed by the campus or department as necessary for use in connection with Fabens ISD business. A student's email should be deleted unless otherwise required in connection with Fabens ISD business. In all such cases, the extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose. Campuses and departments are encouraged to make arrangements for the disposition of email files with departing employees and students in advance of their departure.

**Privacy of Data, other than Electronic Mail, Stored on Fabens ISD Computers and Networks**

As is the case with electronic mail, access by authorized Fabens ISD employees to electronic data stored on the district's network of computers may be necessary to ensure the orderly administration and functioning of Fabens ISD’s computing systems. Such access may require

the employee gaining access to the data to read specific files. The district requires system administrators and other employees who, as a function of their jobs, routinely have access to electronically stored data, to sign statements agreeing to maintain the confidentiality of such information.

In order to conduct its business without interruption, the district must have access to data stored on Fabens ISD computers and networks. Accordingly, for legitimate business purposes, campus principal or department supervisor may in his or her discretion authorize the accessing or retrieval of any files other than electronic mail stored on Fabens ISD computers under that campus or department's control, where necessary and appropriate, Fabens ISD network support personnel may assist with retrieval of such information on behalf of a campus principal or department supervisor, even if the information is stored at a site other than the campus or department's computer systems.

There is no guarantee of privacy or confidentiality for documents or data stored on Fabens ISD-owned equipment.

**Public Records Considerations**
Electronic mail and other data stored on Fabens ISD computers may constitute a public record like other documents subject to disclosure under the Texas Public Records Act or other laws, or as a result of litigation. However, prior to such disclosure, the district evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law. All email will be stored on the Fabens ISD servers for a time period of one year. Incidental personal electronic mail may be destroyed at the user's discretion.

**Conclusion**
Wherever possible in a public setting, individuals' privacy should be preserved. However, there is no guarantee of privacy or confidentiality for data stored or for messages stored or sent on Fabens ISD-owned equipment. Persons with questions about the applicability of this Policy to specific situations should contact the Fabens ISD Technology Department.

Violations of Fabens ISD policies governing the use of Fabens ISD electronic resources, including mail services, may result in restriction of access to Fabens ISD information technology resources in addition to any disciplinary action that may be applicable under other Fabens ISD policies, guidelines or implementing procedures, up to and including dismissal. Suspected violations of Fabens ISD Policy may be reported to the Fabens ISD Technology Director.

# V. Technology Help Desk

The Fabens ISD Technology Help Desk is accessible through the Fabens ISD Technology Department website.

# VI. Remote Management Guidelines

**Introduction**

FISD Technology Department added remote management as a method of providing desktop support to end users on campus. Using these tools, computer support staff members are able to interact with the end user's computer system without having to physically visit the end user's office. While not every computer problem can be resolved remotely, there are a large number of software installations and application support tasks that can be performed without needing to be physically present at the computer.

These guidelines describe the use of remote management of desktop PCs. Procedures to accept a remote management connection as well as to terminate the connection are described.

**Privacy Concerns**

It is understood that some users on campus will have concerns regarding privacy and the security of data located on their system. These issues are addressed in a number of different ways:

- The remote management agent software is configured so that the end-user must explicitly give staff member's permission to remote access their computer each and every time the remote management tools are used.
- The Fabens ISD Acceptable Use Policy outlines the obligations of authorized support staff in regard to maintaining the privacy and security of user files, data, and mail. These obligations apply regardless of what method the staff uses to provide computer support.
- The remote management agent software is a component of the Novell client software. As the software is not as commonly used as other remote management solutions, it is less likely to be the target of random attacks and hacking activity. Additionally, computer support personnel who wish to use the remote management tools must be authenticated and logged into the Novell servers on campus, providing end-users confidence in who is really trying to remote manage their systems.
- Remote management can only occur on systems running the remote management software. When this software is running, an icon will be visible in the system tray located at the bottom right-hand corner of the screen. To determine if the Novell remote management agent is running on your computer, check for this icon.
- Right-clicking on this remote management icon can access additional Information regarding remote management on your computer.

**Establishing and Authorizing a Remote Access Session**

An authorized Support staff member will ask you to request a remote management session. You can do this as follows:

- Right-click on the Remote Management icon in your system tray.

- Left-click on 'Request Session'
- A 'Request Session' window will appear. In the Console window, enter the IP address that the support staff person just provided to you. In the operation field, you can select either Remote Control or Remote View. If you select Remote View, the computing support staff person will only be able to see what you do and will not be able to take any action on your behalf.
- You will see a window appear on your computer screen that requests permission to perform a specific remote management function on your computer. The fully distinguished Novell user name of the person who wishes to control your machine is displayed (.admin.info in the examples). If you are expecting someone to remotely access your computer you can answer yes. If you are not expecting one of these windows to appear or if you do not recognize the username of the person requesting access then you can answer no. If you answer NO the remote management session is refused and remote access to your computer will not be allowed.
- Once you click **Yes**, the session is established.

**Working in a Remote Management Session**

When a remote control session is established, a status bar will be displayed in the upper right-hand corner of your computer screen. You can also use the Remote Management icon in the system tray to see if you are being remotely managed (and by whom). You can terminate the remote session by clicking on the X in the status bar. You can also terminate the remote session using the menu from the Remote Management icon in your system tray.

The contents of the screen information transferred between systems are encrypted which results in a minor decrease in responsiveness during the remote control session.

**Frequently Asked Questions:**

**Q.** *Can you take control of my computer while I'm gone for coffee, lunch, or otherwise away from it?*

***A. No. The remote control must be authorized. The remote management agent is configured so that a user must be present at the computer that is to be controlled to grant access.***

**Q.** *Can you gain access to my machine through remote management without me granting permission every time?*

***A. No. Permission must be granted each time.***

**Q.** *Can my supervisor, coworkers, or colleagues use these remote management tools to spy on me?*

***A. No. Only authorized computer support staff has the required security permissions to initiate a remote management session. Even if they did have permission you would have to authorize the connection.***

**Q.** *Can support staff lockout my keyboard and mouse while they are controlling my machine?*
***A. No. The ability to lock out an end user's keyboard and mouse during a remote control session has been disabled. However, end-users are advised that they should not attempt to use their computer for any purpose while computer support staff is working on it remotely. Even doing something as simple as launching Netscape or checking your email while a technician is loading software could result in a failed installation that requires even more time to fix.***

**Q.** *What should I do if I need to use my computer while it is being remotely managed?*
***A. Please contact the person who is remotely managing your machine before you attempt to use it. They will be able to tell you if it is safe to use and ensure that you do not inadvertently do any damage to your system.***

**Q.** *How will I be able to tell when a remote management session is complete?*
***A. During a remote management session, a status bar will be present in the upper right-hand corner of your computer screen. When this status bar disappears, the remote management session has been terminated. Computer support staff may also phone to inform the user of the results of the remote management session.***

**Q.** *In the remote management information, how long is the remote management history stored?*
***A. The remote management history can be viewed from the information screen of the remote management icon located in the system tray. This history is only preserved for the current windows session and is reset every time you reboot your computer. Unfortunately, this is not a configurable setting and there is no way to make it preserve the history between reboots.***

# VII. Asset Inventory Management System

This database is designed to maintain an inventory of all technology equipment. In order to maintain accurate records, any relocating of equipment will be performed by the Technology Department. The advantages of maintaining accurate records are better service to the campuses/departments, prevention of time lost by technology staff by eliminating the need to track down the correct inventory information, and the ability to plan and prepare. Each Location Identification Bar Code Tag indicates a physical location in the campus/department. Each number is unique for that equipment. If your equipment is not labeled, please report this to the FISD Technology Department.

# VIII. Equipment Repurposing Guidelines

All computers are purchased with three-year warranties. The repair/life cycle support for all district-approved computer equipment is for a period of five years if parts are available from the vendors. In the event of equipment failure after five years, the computer should be processed for disposal.

### Parameters for the repurposing of older equipment:

Computers that have exceeded their life cycle (i.e. 5 years old or older) **AND** are being considered for replacements as part of a District, Campus, or Department initiative may be repurposed in a stand-alone configuration **OR** tagged for disposal.

- No network connectivity will be provided.
- Minimal district-level support or repair will be provided.
- No campus or district funds will be expended to purchase software or hardware upgrades for these computers.
- The disposal of old computers will be at the discretion of the FISD Technology Department. FISD Technology Department will use the machines for parts when possible and will be responsible for removal from inventory.
- The department/campus administrator and the Technology Director must approve all requests for new workstations that do not replace an existing machine.

Computers that have exceeded their warranty, but not their life cycle (i.e. in their 5$^{th}$ year) **AND** are being considered for replacements as part of a District, Campus, or Department initiative may be repurposed in a stand-alone configuration **OR** tagged for disposal.

- No network connectivity will be provided.
- District-level support and repair will be provided.
- It is highly recommended that no campus or district funds be expended to purchase software or hardware upgrades for these computers.
- The disposal of old computers will be at the discretion of the FISD Technology Department. FISD Technology Department will use the machines for parts when possible and will be responsible for removal from inventory.
- The department/campus administrator and the Technology Director must approve all requests for new workstations that do not replace an existing machine.
- It is a campus responsibility to fund upgrades and, if necessary, upgrades to the hard drive and/or memory to support the new OS.
- The department/campus administrator and the Technology Director must approve all requests for new workstations that do not replace an existing machine.

# IX. Equipment Disposal Guidelines

All equipment purchased is considered the sole property of Fabens ISD. Therefore, it is required that old, expired or unneeded equipment be returned to the Fabens ISD Technology Department unless special arrangements have been made. This is also required of newer equipment, in the event that an employee leaves the school district.

The custodian of the equipment will submit a Technology Work Order ticket to have the equipment removed from their classroom or office.

The technician will verify whether the equipment is currently under warranty, and assess its working condition. The technician will record this and all other relevant information on an accompanying work order that will assist the Technology Director or assigned personnel in determining how to allocate the equipment.

In general, working computers which are covered by a warranty, and which fall within the minimum FISD operating standards will be retained for future use pending the destruction of all data from the system.

Machines that are retained will fall under the ***Repurposing Guidelines*** for the district.

For non-working computers that are still covered under warranty, the technician will call the vendor to repair or replace the equipment so it can be reused. Inoperable equipment no longer under warranty will be processed for disposal. When equipment becomes obsolete, damaged, or broken beyond reasonable repair, it will be properly disposed of according to district guidelines.

Working machines that do not meet the minimum FISD operating standards or that are past the warranty will be stored for district surplus sales to the community.

# X. Equipment Checkout Guidelines

Equipment is defined as any computer, projection device or other peripheral made available for checkout. The primary intent of checking out equipment is in support of presentations and training conducted by faculty outside of the school district. Equipment will not be loaned for extended periods of time so as not to hinder others access to this resource. The Technology Director may make exceptions.

**Responsibility:**

- Responsibility for the equipment lies with the Borrower from the time the equipment is released until the equipment is checked back into the Technology Department. ***ALL REASONABLE SECURITY TO PREVENT THEFT OR DAMAGE IS THE RESPONSIBILITY OF THE BORROWER.***
- All returned equipment would be inventoried and checked for damage upon return. If damage has occurred and if repair or replacement is necessary the borrower will be notified and the borrowers will be responsible for any fees incurred due to repairs of the equipment. Use the checkout form equipment inventory list to ensure all equipment and accessories are accounted for before returning to the Technology Department.
- Equipment setup and takedown is the responsibility of the borrower.

**Usage:**

- ***Hardware:*** Hardware may not be added or removed from the original configuration without the express permission, in writing, from the Technology Director.
- ***Software:*** Approved and licensed software will be pre-loaded onto all computers. If non-standard software is to be loaded, this should be indicated on the equipment checkout requirements and the borrower must provide appropriate license(s) and media. Software loaded onto the equipment at a training site must be removed or uninstalled in an acceptable manner before leaving that site.

**Check out procedure:**

- Equipment checkout is on a ‘first-come' basis and should be reserved at least two weeks in advance of the need.
- Equipment checkout is facilitated through the Technology Department office the equipment checkout form must be completed.
- The Check-Out date is the date equipment will be available for pickup. The Check-In date is the date equipment must be returned.
- Equipment can be picked up and returned to the Technology Department.

# XI. Hardware & Software Purchasing Guidelines

The purchase and/or upgrade of Technology Hardware and Software, as well as related services, must be consistent with the District’s strategic technology planning objectives and activities contained in the ***Fabens ISD Technology Plan***. All technology equipment and software purchases and/or upgrades must meet the minimum established District standards. In order to ensure proper hardware configuration, hardware and/or software compatibility, as well as technical support, **all technology purchases** must adhere to the following requirements:

The purchase of instructional software and/or equipment must be coordinated with the technology department.

- The Principal must submit a Hardware/Software Purchase Request Form or Director's designee form is available on FISD Technology home page.
- All Hardware/Software purchases will require a technical evaluation, which will be performed by the FISD Technology Department prior to purchase.
- The campus/department's purchase requisitions must reference a Software/Hardware Purchase Request Form and the Technology Director's signature.
- The campus or department must obtain pricing from the Technology Department's established bid/quote process. The vendors and prices have been approved by the District's Purchasing Department.

# XII. Software Copying

FISD employees must adhere to the following stipulations:

1. No copies of software may be made except in the following cases:
    - Normally an archive copy of the software is allowed for protection against accidental loss or damage. Archive copies of software should be securely stored and not used except to be re-copied if the operational copy becomes damaged.
    - Some software, when site licensed by the producer, may permit unlimited copies for use within the District. Such copies must be made only by the person or persons authorized to make copies by the terms of the site license. In this case, duplicates shall be clearly labeled as District copies of the licensed software.
    - Some software, in particular, programming languages, allow code to be copied and incorporated within user-written software. Such use is generally permitted as long as the software is for personal use and not sold, rented, or leased.

1. If the distribution or commercial use is intended for the software so produced, clearance must be secured from the copyright owner for use of the incorporated code and from the district for the use of the equipment during the production.
2. The intended or unintended piracy, damage, alteration, or removal of any district-acquired software may be treated as an act of theft or malicious destruction. The district may elect not to extend computer services to persons who have been identified as engaging in these acts.
3. The user is responsible for complying with whatever terms or conditions are specified in the license agreement or copyright statement, which accompanies individual software acquisition.
4. Be aware that unless it has been verified that the software you are using is covered under a site license, no copying is allowed.

5. Be aware that the district technology department reserves the right to inspect software stored or used in its computers. Inspections conducted by the Technology Department will be undertaken only after there is evidence or concern that an employee or volunteer is in violation of these guidelines. Should inspection prove necessary, it must be unannounced and unscheduled to be effective.
6. To ensure individual privacy, however, the following conditions shall be met:
    - The individual employee must be present for the duration of the inspection.
    - A member of the FISD Technology Department must do an inspection.
    - Software only may be inspected. The contents of data or textual files shall not be examined or reviewed.

# XIII. Donated Technology Equipment and/or Software Guidelines

All technology equipment and software that is being donated for use on the District's computers and/or network must be certified by Technology Director as "compatible" with the minimum technology standards, and as "supportable" to ensure appropriate maintenance and repair.

# XIV. Disaster Recovery Plan

The purpose of the Fabens ISD Disaster Recovery Plan is to provide for the continuation of the information processing and telecommunications required supporting Fabens ISD should a disaster occur affecting the necessary computing and telecommunications systems. This plan provides recovery personnel with the information required in implementing the disaster recovery effort. It provides the necessary information and procedures to facilitate the recovery from a disaster and to relocate computing and telecommunications equipment, if necessary, to a recovery center at the time of a disaster.

# XV. Power Off Computers Guidelines

All staff members are reminded to turn off the power to their desktop computers at the end of the workday. Note that the power is still on for a computer even when it is "asleep" in energy-saving mode, switch the surge protector to "off" to ensure that all power to the computer is disconnected. Exceptions: computers scheduled for automatic backup during the night, computers that are running critical processes at night, and computers explicitly configured for remote access. At the end of your workday, please be sure to completely shut down your computer and turn the power off via the switch on the computer or via the surge protector.