FRENCHTOWN SCHOOL DISTRICT NO. 40
P.O. BOX 117
FRENCHTOWN, MONTANA 59834

Les Meyer
406-626-2600
FAX 406-626-2605
Superintendent

JAKE HAYNES
406-626-2670
FAX 406-626-2676
High School Principal

AARON GRIFFIN
406-626-2650
FAX 406-626-2654
Middle School Principal

RILEY DEVINS
406-626-2622
FAX 406-626-2623
Intermediate Principal

JODI HALL
406-626-2620
FAX 406-626-2625
Elementary Principal

JENNIFER DEMMONS
406-626-2775
FAX 406-626-2605
Special Services Coordinator

SHAUNA ANDERSON
406-626-2706
FAX 406-626-2605
District Clerk

ACCEPTABLE USE OF TECHNOLOGY POLICY

Table of Contents

1.0 Purpose

The purpose of the Acceptable Use of Technology Policy is to define the standards for the acceptable use of Frenchtown School District #40 computing equipment, internet, information, and communications

2.0 Scope

This Policy applies to all of Frenchtown School District employees, contractors, vendors, agents, consultants, temporary workers and any other person or entity who has access to or connects to any of Frenchtown School Districts electronics, network, or other electronic resource or who utilize any computing or other equipment

owned, leased or managed by Frenchtown School District or any equipment that is connected to the Network. This Policy governs all access including local, remote, and mobile access to the Network.

3.0 Policy

The requirements contained herein are cumulative and are meant to be read in conjunction with one another and not in isolation.

3.1 General Guidelines

1. **ALWAYS** exercise common sense and good judgment.
2. Access to the network is a privilege, not a right. Access may be suspended at any time and for any reason. Frenchtown School District reserves the right to monitor, audit and police the use of its Network and any content or communication stored on or communicated through the Network. Your use of the Network or the equipment constitutes your consent to this monitoring.
3. Any data or other Information created or stored on the Network or any Equipment becomes and/or remains the property of Frenchtown School District.
4. Frenchtown School District may modify this Policy without notice.
5. Units, departments, and groups may establish more restrictive policies for their respective users but may not waive or lessen any requirement contained in this Policy without written authorization from the Information Technology department or its designee. Any such more restrictive policy must be in writing and must be made available to that unit, department or group that is subject to the additional restrictions.
6. In accordance with Frenchtown School District you should have no expectation of privacy in any location, item, information or communication existing or occurring on or in FTSD property or when using FTSD resources or equipment, even if protected by passwords, access codes, keys, locks or other security devices.
7. At the end of your employment or service, you are required to relinquish all Frenchtown School District owned, leased or managed Equipment and all files or Information in an unencrypted, non-password protected and readily accessible form. You may not attempt or continue to access the Network or Equipment after the end of your employment or service.
8. **ALWAYS** follow all applicable policies.

3.2 Equipment/Hardware

1. **NEVER** connect personal equipment to the Network without authorization from FTSD IT.
2. **NEVER** remove Equipment from FTSD premises without authorization. Employees who are issued laptop computer or other Portable Storage Devices that are intended to be removed from the premises are presumed to have authorization unless otherwise instructed.

3. **NEVER** knowingly perform an act which will interfere with the normal operation of FTSD Network and Equipment.
4. **ALWAYS** have up to date anti-virus software installed and running on all Equipment connected directly or remotely to the Network.
5. **ALL** Equipment connected to the Network must meet the minimum requirements established by FTSD Information Technology Department.
6. Except as otherwise provided, **ALWAYS** store all FTSD Information on your assigned FTSD network home drive a department network shared drive.

3.3 Portable Storage Devices

Portable storage devices are especially susceptible to being lost or compromised and additional requirements must be followed. The following are some general requirements followed by additional specifications for particular types of Portable Storage Devices. Portable Storage Devices are divided into five broad categories: (1) laptops and mobile computers, (2) CD/DVD/Disk, (3) external hard drives (including removable hard drives and USB thumb/flash drives), (4) backup tapes, and (5) handheld/wireless devices.

A. General Requirements

1. **NEVER** leave any portable storage devices unattended and unsecured. When a device is left unattended, it should be protected as much as possible against unauthorized access or removal (e.g., locked in a cabinet, drawer, hotel room safe, cable locked or otherwise protected from unauthorized removal).
2. **NEVER** leave any Portable Storage Devices in any vehicle overnight. Never leave a device unattended in a vehicle unless it is protected as much as possible against unauthorized access or removal (e.g., locked in the trunk or, if the vehicle does not have a trunk, in a location that is not visible from outside the vehicle).
3. **ALWAYS** immediately report all lost or stolen Portable Storage Devices to FTSD Information technology department by email or IT ticket request.
4. **ALWAYS** comply with the instructions and requests of those assigned to investigate the lost or stolen Portable Storage Device.
5. **ALWAYS** take precautions to prevent your login, password, and any FTSD Information from being viewed by others while using a Portable Storage Device.
6. Except as otherwise provided herein, **NEVER** save FTSD Information or other files on your Portable Storage Device other than those files automatically saved on it by the device's applications or necessary to run the Portable Storage Device.
7. **NEVER** store any student or sensitive FTSD Information on any Portable Storage Device, in accordance with this Policy.

D. External Hard Drives (including USB thumb/flash drives)

1. **NEVER** store/save RESTRICTED or SENSITIVE Information to external hard drive without FTSD Information Technology Department's review and written approval.
2. **ALWAYS** encrypt all SENSITIVE FTSD Information saved to an external hard drive in accordance with FTSD Encryption Policy.
3. **ALWAYS** encrypt or password protect all RESTRICTED FTSD Information saved to an external hard drive.
4. You may store FTSD Information that is NOT SENSITIVE or RESTRICTED but has a legitimate business purpose to an external hard drive without encryption or password protection.
5. **NEVER** save any information that does not have legitimate business purposes to any external hard drive using FTSD Network.

F. Handheld/Wireless Devices

1. **ALL** Handheld/Wireless Devices must be password protected, including personal devices containing any Information.
2. **NEVER** send to or save any RESTRICTED or SENSITIVE FTSD Information to a Handheld/Wireless Device unless it is protected in accords with FTSD Information Security Policy.

3.4 User IDs & Passwords

1. You are responsible for the security and confidentiality of your passwords and account access. If your password is lost, stolen or if its integrity is compromised immediately alert FTSD Information Technology Department.
2. **ALWAYS** change your password(s) at least once a year
3. **ALWAYS** use a strong password that is at least ten (10) alphanumeric characters in length, uses "special" characters in addition to numbers and letters (e.g., !@#$%^&*()_+|~), and uses both upper and lower case characters (e.g., a-z, A-Z). Do not base password off of any personal information (e.g., date of birth, name) or that are words any language, slang, dialect, jargon, etc. Never use common or generic usernames or passwords (e.g., admin or password).
4. **NEVER** reveal your password to any other person, at any time, for any reason. This includes your supervisor, co-workers, vendors, or third-parties such as family and other household members. FTSD Information Technology staff will NEVER ask for your password.
5. **NEVER** write down or store your password in an unprotected fashion or transmit it via e-mail or another form of unencrypted communication.
6. **ALL** passwords must be deleted or changed immediately upon the end of employment or service for any User.
7. **ALWAYS** review your level of access (including which systems and applications you have access to) whenever your responsibilities, function or position changes. It is the obligation of every User to make sure that their level of access is current.
8. **ALL** User-, system- and application-level passwords must conform to FTSD Password Policy.

3.5 Illegal or Prohibited Activities

1. **ALWAYS** comply with all applicable laws, and all FTSD policies.
2. **NEVER** violate any rights protected by copyright, trade secret, patent or other intellectual property, or similar law or regulations.
3. **NEVER** make any unauthorized use, duplications, broadcast or sharing of any content, in any form, that is subject to any copyright or other restriction and for which FTSD or the User does not have the appropriate license.
4. **NEVER** allow anyone else to use your username or password to log onto the network or any application.
5. **NEVER** use equipment or an account that you are not authorized to use or obtain a password without the consent of the account owner.
6. **NEVER** use the Network to gain unauthorized access to any computer system.
7. **NEVER** attempt to circumvent data protection mechanisms, content filters or uncover security flaws.
8. **NEVER** use any software/application that has not been approved by FTSD Information Technology department or violate the terms of any applicable software licensing agreements or terms of use.
9. **NEVER** mask the identity of an account or machine without authorization.
10. **NEVER** attempt to monitor or tamper with anyone's electronic communications, or read, copy, change or delete anyone's files or software without authorization.
11. **NEVER** export software, technical information, encryption software or technology to foreign countries or nationals in violation of export control laws.
12. **NEVER** knowingly introduce or disseminate any malicious programs or code (e.g., virus, worm, Trojan horse, e-mail bomb, etc) into or on the Network.
13. **NEVER** access, procure or transmit any material or content in violation of FTSD policy or that creates a hostile work environment.
14. **NEVER** use the Network or Equipment to search for, access or otherwise utilize any site, service or content related to gambling or gaming, adult material or content, that disparages any racial, ethnic, religious or other group in violation of FTSD policies, or unauthorized social networking sites (including online dating).

3.6 Electronic Communications

The following are additional requirements that apply to Electronic Communications. The term Electronic Communications includes but is not limited to e-mail, text messages, instant messages, telephone calls or any other type of analog or digital communication sent over or using the Network or using any Frenchtown School District Equipment.

1. **ALWAYS** exercise caution when opening e-mail attachments received from unknown or untrusted senders.

2. **NEVER** distribute unsolicited e-mail messages including sending of "junk mail" or other advertising material when outside your scope of responsibility.
3. **NEVER** distribute "chain letters," "Ponzi" or other "pyramid" schemes of any type.
4. **NEVER** make or send harassing e-mail, telephone calls or other messages whether through language, frequency, or size of messages.
5. **NEVER** introduce sexually explicit or otherwise offensive material into any electronic communication or other medium unless this activity is a part of the User's authorized job or duty.
6. **NEVER** use unauthorized or forged e-mail header information.
7. **NEVER** email unencrypted sensitive information, including but not limited to social security numbers, driver's license or state-issued identification numbers, financial account numbers or credit/debit card numbers.
8. **NEVER** use non-FTSD e-mail, instant messaging or other communications services not approved by FTSD IT Department to conduct company business.

4.0 Reporting Breaches in Security

Reporting Breaches in Security

If you observe or suspect any type of suspicious, abnormal or unauthorized activity that threatens the integrity, confidentiality or availability of FTSD Network or Equipment; or any activity that compromises or is likely to compromise student or staff personal information, whether through unauthorized disclosure, access, or destruction, you should immediately contact your Administrator and report the incident to the Information Technology department.

5.0 Enforcement

Any violation of this Policy may result in termination of your use or access to the Network and/or disciplinary action up to and including termination. FTSD may take any legal action it deems appropriate and/or report any suspected unlawful conduct to law enforcement.

FRENCHTOWN SCHOOL DISTRICT NO. 40
P.O. BOX 117
FRENCHTOWN, MONTANA 59834

Les Meyer
406-626-2600
FAX 406-626-2605
Superintendent

JAKE HAYNES
406-626-2670
FAX 406-626-2676
High School Principal

AARON GRIFFIN
406-626-2650
FAX 406-626-2654
Middle School Principal

RILEY DEVINS
406-626-2622
FAX 406-626-2623
Intermediate Principal

JODI HALL
406-626-2620
FAX 406-626-2625
Elementary Principal

JENNIFER DEMMONS
406-626-2775
FAX 406-626-2605
Special Services Coordinator

SHAUNA ANDERSON
406-626-2706
FAX 406-626-2605
District Clerk

Password Policy

1.0 Purpose

The purpose of this policy is to define a standard for the creation of strong passwords. These standards will also define the methods utilized to protect the passwords and indicate the recommended frequency of change for all passwords regarding Frenchtown School District information resources.

2.0 Scope

This policy applies to all Frenchtown School District employees, contractors, vendors and agents with a Frenchtown School District -owned or personally owned computer used to connect to any portion of the Frenchtown School District network. This policy also provides coverage for applications as well as systems that provide access to Frenchtown School District information resources.

3.0 Policy

3.1 General

- Initial passwords are unique and must be changed during an authorized user's initial login.
- All passwords (e.g., e-mail, web, desktop computer, etc.) must be changed every 12 months.
- Passwords must not be revealed to others. This includes family and other household members when work is being done at home.
- Passwords must not be inserted into e-mail (IT departments may send temporary passwords via email or via other methods of communication) or other forms of unencrypted communication.
- Administrative accounts must be protected at the highest level of vigilance. Administrative passwords must be deleted or changed immediately upon termination of any employee with access to administrative accounts.
- Personal accounts must be deleted at time of termination.
- All user-level and system-level passwords must conform to Frenchtown School District Password Standards.

- Passwords used in any application or script must also conform to Frenchtown School District Password Standards.

For account set-up or password resets, contact the Frenchtown School District IT department @ 406-626-2608

3.2 Password Standards

Passwords are used for various purposes within Frenchtown School District. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, voicemail password, and local router logins. All authorized users should be aware of how to construct a password.

Passwords should have the following characteristics:

1. Be at least ten alphanumeric characters in length
2. Contain "special" characters in addition to alphanumeric characters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
3. Contain both upper and lower case characters (e.g., a-z, A-Z)
4. Are not based on personal information, names of family, etc.
5. Are not words in any language, slang, dialect, jargon, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "this may be one way to remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation of the phase. Another method is to take two words and separate them with special characters such as word&&word.

Examples of unacceptable or "weak" passwords include the following:

1. The password contains less than eight characters
2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc., birthdays and other personal information such as addresses and phone numbers, word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc., any of the previously mentioned words spelled backwards, any of the above preceded or followed by a digit (e.g., secret1, 1secret).

4.0 Enforcement

If an account or password is suspected of being compromised, please report the incident to Frenchtown IT department technology@ftsd.org and immediately change the password in question. Frenchtown IT department may perform password audits on a periodic or random basis. If a password is identified, the owner will be immediately notified and required to modify the password. Any employee or third parties found to have violated these standards may be subject to disciplinary action and/or legal action, including termination of employment, termination of access to Frenchtown School District systems and/or networks and subsequent criminal/civil prosecution.