INFORMATION TECHNOLOGY

Cellphone Purchases

The Fort Vermilion School Division participates in a GOA plan that has been negotiated with Telus. As such, all cellphones are purchased outright and are not connected to a cellphone/data plan. The purchasing of cellphones is guided by the following principles;

- All cellphones are purchased via the IT Department.
- Unless lost or no longer functioning appropriately as determined by the IT Manager, cellphones are not replaced for at least three years and may be utilized longer if working properly.
- The cost of purchasing cellphones are borne by schools or departments.
- Damaged cellphones will be replaced where possible with a refurbished model. Replacement costs will be borne by the school or department. Refurbished models will not be replaced for a minimum of two years. The IT department will make the decision as to whether a cellphone will be replaced by a refurbished cell phone or a new cell phone.
- Cellphone purchases, years in service and usage tracking is the responsibility of the IT Department.

Deletion of Accounts

All Fort Vermilion School Division computer accounts are subject to the following guidelines for removal of accounts:

- Staff that are leaving the jurisdiction will have their computer account remain active for a period of two weeks from the end of school.
- At that time accounts will be suspended and not accessible. If a staff member notices that something was missed during the two weeks above, staff will need to contact the IT department to re-open the account.
- Accounts will be removed two weeks after initial suspension. Once deleted, accounts are no longer accessible and cannot be re-activated. NOTE: This is two weeks after initial suspension, should an account be re-activated the two week period does not restart.
- Student accounts will be automatically suspended at the time they are removed from the SIS system.
- 30 days from the time of suspension student accounts will be deleted.
- Central Office executive staff accounts will remain in suspension for six months prior to removal of account.

For the purpose of clarification, suspension/deletion of accounts means that users will no longer be able to access files, folders, email or contacts.

Digital Citizenship Instruction

Each school will ensure that all FVSD students receive ongoing Digital Citizenship instruction throughout the school year using resources developed by the technology committee. These resources are found in the FVSD Admin Centre. When necessary these resources can be modified to ensure the contents are appropriate for the cultural sensitivities of each community. Teachers / schools are encouraged to provide additional Digital Citizenship instruction as needed depending on the level of use of digital tools and apps. Supplementary resources can also be found in the FVSD Admin Centre.

FVSD Guidelines for All Technology Uses for Staff

Administration will review **the Information Technology Acceptable Use Protocol, Password Protocol and Messaging Protocol with staff** at the beginning of each school year and as needed throughout the year. All staff will read and sign the **FVSD Guidelines for All Technology Uses for Staff and FVSD Staff Technology User Agreement** (FVSD Forms).

FVSD Guidelines for All Technology Uses for Students

Teachers will review the **FVSD Guidelines for All Technology Uses for Students and FVSD Student Technology User Agreement** (FVSD Forms) as well as the **FVSD Student Internet Use Guidelines, User Agreement and Parent Permission Form** (FVSD Forms – Student Registration Form) with students annually and as needed throughout the year. **The FVSD Student Internet User Agreement and Parent Permission Form** will be signed by the student and the parent **annually** before students are given access to the Internet. These will be kept on file at the school.

While involved in instruction, all students are prohibited from using personal technology devices unless approved by the principal for instructional purposes and/or included in the student's instructional support plan (IPP). In high school, students are permitted to appropriately use personal devices before or after school and during recess and non-instructional blocks. The Fort Vermilion School Division has provided all technology devices needed for learning. A student who breeches this guideline may receive disciplinary action as per the FVSD Student Code of Conduct and the School's Student Code of Conduct.

Information Technology Acceptable Use Protocol

Overview

The Acceptable Use Protocol is not intended to impose restrictions that are contrary to Fort Vermilion School Division #52's (FVSD) established culture of openness, trust and integrity. The Fort Vermilion School Division is committed to protecting its employees, students, partners and the division from illegal or damaging actions by individuals, either knowingly or unknowingly.

All school division owned information technology resources are to be used for educational purposes in serving the interests of the division and of our students and staff in the course of normal operations.

While involved in direct instruction with students, all staff are prohibited from using personal technology devices unless approved by the Principal for instructional purposes. The Fort Vermilion School Division has provided all technology devices needed for instruction. An employee who breaches this guideline may receive disciplinary action up to and including dismissal. Principals and Vice-Principals are expected to carry their FVSD cell phones throughout the day; however, they should only be used for emergencies while involved in direct instruction with students.

Staff are permitted to use personal technology devices when not in direct instructional or supervisory capacity of students.

Should supervision of students be outside the regular school day, when active supervision is not required, staff need to employ appropriate judgment when using personal technology devices. Examples of active supervision may include, but not be limited to swimming, coaching and higher risk activities. An example of passive supervision would be supervising students on a bus ride.

Effective security is a team effort involving the participation and support of every FVSD employee, student and affiliate who deals with information and/or information systems. It is the responsibility of every information technology user to know these guidelines and to conduct their activities accordingly.

Purpose

The purpose of this protocol is to outline the acceptable use of information technology equipment and FVSD information technology resources, including division owned as well as personally owned or other digital devices. These guidelines are in place to protect the student, employee and FVSD from risks associated with inappropriate use.

Scope

This protocol applies to employees, students, contractors, consultants, temporaries, and other workers at FVSD, including all personnel affiliated with third

parties. All equipment and resources owned or leased by FVSD as well as personally owned devices are covered by this protocol. It will also encompass activities outside normal school operations and property where there is a negative impact.

Protocol

General Use and Ownership

1. FVSD expects that all users of FVSD technology resources and personally owned digital devices will adhere to the elements of digital citizenship. All users will advocate and practice safe, legal, and responsible use of information and technology that supports collaboration, learning, and productivity.
2. While FVSD's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of FVSD. Because of the need to protect FVSD's network, management cannot guarantee the confidentiality of information stored on any network device belonging to FVSD.
3. Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty as to reasonableness, employees should consult their supervisor or manager; students should consult their teacher.
4. For security and network maintenance purposes, authorized individuals within FVSD may monitor equipment, systems and network traffic at any time.
5. FVSD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this protocol.

Security and Proprietary Information

1. All passwords will conform to the Password Protocol.
2. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by manually locking or logging-off when the host will be unattended.
3. All division owned portable digital devices will be password protected and will automatically lock after a period of inactivity.
4. All personally owned portable digital devices accessing FVSD data will be password-protected and will automatically lock after a period of inactivity.
5. Lost or stolen division owned portable digital devices shall be reported to the IT Department immediately.
6. Because information contained on portable digital and external storage devices is especially vulnerable, special care should be exercised to ensure the security of the data.
7. All devices used by the employee and student that are connected to the FVSD network, whether owned by the employee, student or FVSD, shall be running an up-to-date security program.

8. Employees and students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horse code or other undesired content. Users should contact the Information Technology department for information on how to handle these issues.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee or student of FVSD authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing FVSD and/or personally owned or other resources.

The lists below are by no means exhaustive, but they attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited with no exceptions:

1. Violations of the rights of any person or division protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by FVSD.
2. Using an FVSD device to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
3. Engaging in cyber bullying in any form.
4. Providing information about, or lists of, FVSD employees or students to parties outside FVSD.
5. The placing of unlawful information on the Internet.
6. Accessing hate literature or other media deemed unacceptable.
7. Accessing any form of pornography, written or visual, at any time.
8. Accessing any information of which the use would be deemed illegal in Alberta or Canada.
9. The use of abusive or otherwise objectionable language in either public or private messages.
10. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Students may share account information with their parents or guardians.
11. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any

copyrighted software for which FVSD or the end user does not have an active license.

12. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
13. Making fraudulent offers of products, items, or services originating from any FVSD account.
14. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or student is not an intended recipient or logging into a server or account that the employee or student is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, packet spoofing, denial of service, and forged routing information for malicious purposes.
15. Port scanning or security scanning is expressly prohibited.
16. Executing any form of network monitoring which will intercept data not intended for the employee's or student's device, unless this activity is a part of the employee's or student's normal job/duty.
17. Circumventing user authentication or security of any device, network or account.
18. Interfering with or denying service to any user (for example, denial of service attack).
19. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.

Email and Communications Activities

1. All email access as well as other digital forms of communication shall be governed by the Messaging Protocol.

Student Internet Use

1. All student Internet use shall be governed by the FVSD Student Internet Use Guidelines and User Agreement.

Enforcement

Any employee or student found to have violated this protocol may be subject to disciplinary action, up to and including termination of employment in the case of an employee or expulsion in the case of a student.

Messaging Protocol

Purpose

The purpose of this protocol is to safeguard our students and employees as well as prevent tarnishing the public image of FVSD. When messages go out from FVSD, the general public will tend to view that message as an official policy statement from the FVSD.

Scope

This protocol covers appropriate use of any message sent from an FVSD resource and applies to all employees, students, vendors, and agents operating on behalf of FVSD.

Protocol

Prohibited Use

FVSD resources shall not to be used for:

1. The creation or distribution of any disruptive or offensive messages, including inappropriate language, offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees or students who receive any emails with this content from any FVSD employee or student should report the matter to their supervisor or teacher immediately.
2. Any form of harassment via digital medium, whether through language, frequency, or size of messages.
3. Sending unsolicited messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
4. Unauthorized use, or forging, of email header information.
5. Solicitation of email from an FVSD email account for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Personal Use

Using a reasonable amount of FVSD resources for personal messaging is acceptable, but non-work related messaging should be saved in a separate folder from work related messages. Mass mailings from an FVSD account shall be approved by the FVSD Assistant Superintendent of Operations before sending. These restrictions also apply to the forwarding of messages received by a FVSD employee or student.

Monitoring

FVSD employees and students shall have no expectation of privacy in anything they store, send or receive on the division's network. FVSD may monitor messages without prior notice. FVSD is not obliged to monitor email messages.

Enforcement

Any employee or student found to have violated this protocol may be subject to disciplinary action, up to and including termination of employment in the case of an employee or expulsion in the case of a student.

Password Protocol

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of FVSD's entire corporate network. As such, all FVSD employees and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all staff and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any FVSD facility, has access to the FVSD network, or stores any non-public FVSD information.

Protocol

General

- All staff must select a password that complies with the school division staff password requirements that are distributed internally.
- All students from grade 9 on are encouraged to use strong passwords.
- All students in grades 4 through 8 may use weak passwords.
- All students in grade K through 3 may use weak passwords.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All users must have a unique password.

Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at FVSD. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection and voicemail password. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign language, remember hackers are not only English speaking)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software.
- City, town, province, country, state or continent names 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 above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, 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 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.

B. Password Protection Standards

Do not use the same password for FVSD accounts as for other non-FVSD access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various FVSD access needs. For example, use different passwords for general computer logon and Library logon.

Do not share FVSD passwords with anyone, including administrative assistants, secretaries or IT Staff. All passwords are to be treated as sensitive, confidential FVSD information.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE (this includes the IT Department)
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don’t write it down on a sticky note

If someone demands a password, refer them to this document or have them call someone in the Information Technology Department.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system without encryption.

If an account or password is suspected to have been compromised, report the incident to the IT department and change all passwords.

C. Use of Passwords for Remote Access Users

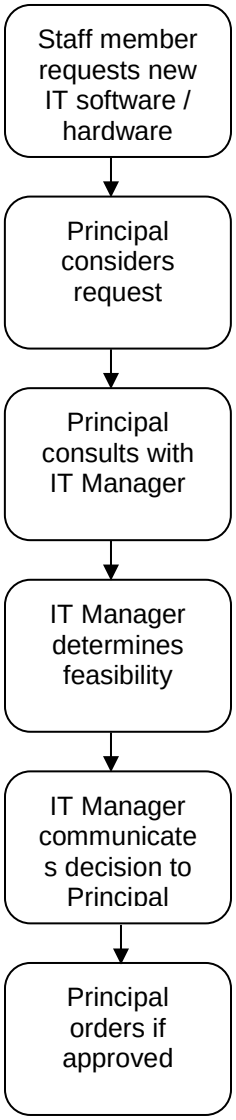
Access to the FVSD Networks via remote access is to be controlled using usernames and passwords.

Enforcement

Any employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment in the case of an employee or expulsion in the case of a student.

Purchase of Information Technology-Related Software and Hardware

Information Technology-related software and hardware that will be connected to the network is **not** to be purchased until **after** consultation between the principal and the IT Manager. Proper authorization from the IT Manager is required to ensure compatibility with the network and compliance with FVSD Information Technology standards. For a summary of current FVSD Administrative Software Programs refer to FVSD Appendices – Summary of Administrative Software Programs.



Social Media Guidelines

For the purposes of these guidelines, social media refers to online technology tools that enable people and organizations to communicate and share information and resources over the Internet. Users provide information, but can also interact with each other using social media. Examples include, but are not limited to blogs, Facebook, Flickr, Instagram, LinkedIn, Pinterest, Twitter, Snapchat and YouTube. Using this definition, the Fort Vermilion School Board's Google platform can also be viewed as social media.

The following guidelines are intended to help staff use social media safely, responsibly and successfully. They align with FVSD board policies and procedures related to the use of technology.

Personal vs Professional

Every time you communicate, whether it's in-person or on social media, you shape public opinion about you, your profession, your school, your board and public education. Statements like, "Tweets are my own and don't reflect my employer's view," don't hold true for educators.

Although staff lead private lives, as such, staff should use sound judgment and due care when using social media while on and off duty.

- Maintain a sense of professionalism at all times - in your personal and professional lives.
- All social media accounts, except official school specific (webpages, Facebook, google classroom) are considered personal in nature.
- Staff should communicate with students for educational purposes only.
- Monitoring posted on your social media account is required in order to ensure the professional image of your online presence.
- Posting images that are considered unprofessional (this includes, but is not limited to inappropriate dress, alcohol, tobacco, etc.) is discouraged on personal accounts.
- If you have a personal social media account that students become aware of, refer them back to the educational account for discussion.
- All pictures of school events, student projects, etc. will be released through official school social media accounts.

Professional Boundaries

Maintaining professional boundaries on social media is critical to sustaining public trust and ensuring relationships with students remain professional. Remember that, on social media, the world is watching.

- All online dialogue and interactions with students should be for educational purposes only.
- Your tone should be formal and professional when communicating with students and others via social media.

- Never share information with students online that would not be appropriate to share in a classroom, or school/community setting. What is inappropriate in the classroom is also inappropriate on social media.
- Your social media interactions should be professional and reflect the board's character attributes: caring, co-operative, honest, inclusive, respectful and responsible.
- Be mindful of all equity and inclusivity-related board policies.
- Keep your posts positive and do not engage in negative or critical conversations online.
- Retweets, likes and favourites are perceived as endorsements. These interactions should be limited and done with care.

Privacy and Confidentiality

Safety is the overriding concern with regard to information posted online. Always respect the privacy and confidentiality of student information. Breaches of privacy and confidentiality can occur with respect to the Municipal Freedom of Information and Protection of Privacy Act, the Youth Criminal Justice Act, and board policies and procedures.

- Ensure privacy settings are appropriate, up-to-date, and protect the privacy and confidentiality of the account.
- Staff must never disclose confidential information about the school, students and colleagues.
- Particular care must be taken with students for whom the principal has identified custody/safety concerns.
- Personal information, including student names, location, etc., should not be posted on social media without informed consent from students' parents/guardians. This includes, but is not limited to blogs, student work, individual and group photographs, videos featuring the student or other identifying information.
- Informed consent is necessary when placing personal student information online. Consent is provided via the blanket consent form that is sent home with all students at the start of the school year.
- Information about school events should be posted on the official school media accounts and then shared by individual users.
- Everything you post can be altered and shared, even if your account is anonymous. Comments expressed privately between social media users can be shared in a more public domain, even with privacy settings set to high.

Professional Hours

Social media operates 24 hours a day, seven days a week. This doesn't mean you have to. Monitoring and replying at any time of the day or night sets up an expectation that you will always do so.

- We encourage schools/staff to establish "professional online hours" and

share them with students and parents so that they know if and when you will respond to questions that are posted on social media.
- Linking to a social media disclaimer is useful in informing the public of the general monitoring of the account. Online hours should be available on your professional social media accounts, e.g. on your Google Classroom, and be strictly adhered to.

Maintenance and Monitoring Responsibilities

At the discretion of the school principal, school social media accounts may be run by one or more school staff members. Communication sent out via social media accounts should have a consistent voice and be positive in tone. Best practice, however, would be that an official school account be updated regularly. If possible, even five minutes a day spent on an account ensures it is considered active and effective.

As well, you are able to respond to questions in a way that is helpful to members of the FVSD community.

- Posts and comments of an inappropriate nature or that contain personal or irrelevant information should be removed/deleted promptly, if permitted by the tool.
- Set your privacy settings so that you are notified if you are tagged or mentioned in photos or posts. Remove tags that may reflect negatively on you.