

FVSD Acceptable Use Policy

— Quick Reference

This is a summary of key points from FVSD's Acceptable Use Policy for technology. All staff are expected to follow these guidelines when using FVSD devices, accounts, and network resources.

Key Points

FVSD Devices and Accounts Are for Work Use

- FVSD computers, email, and accounts are provided for **work and educational purposes**
- Limited personal use is acceptable as long as it doesn't interfere with your duties or violate any policies
- All activity on FVSD devices and networks may be **monitored and logged**

Passwords and Account Security

- **Do not share your password** with anyone — including colleagues, students, and family members when working from home
- **Do not use your FVSD password** for personal accounts or websites
- Lock your computer when stepping away (**Windows key + L**) — FVSD devices are configured to lock automatically after **30 minutes of inactivity**, but you should lock manually whenever you leave your device unattended
- Report any suspected unauthorized access to IT immediately

Mobile Devices

- Any mobile device (phone, tablet) accessing FVSD data through apps like Outlook or OneDrive must have a **passcode, FaceID, or fingerprint** lock enabled
- Only **FVSD-owned devices** may connect to the internal school network — personal devices may only connect to the guest/isolated network

- Any **lost or stolen** FVSD device must be reported to IT immediately

Email and Communication

- Use professional language in all FVSD email and chat communications
- **Do not open suspicious emails** — use the Phish Alert Button to report them (see the [Phishing Awareness](#) article)
- Do not send sensitive student or staff information through unsecured channels

Student Data and Privacy

- Student information is **confidential** — only access records for students you work with directly
- Do not store student data on personal devices or personal cloud accounts
- Follow FOIP (Freedom of Information and Protection of Privacy) requirements when handling personal information

Software and Downloads

- **Do not install software** on FVSD devices — submit a request to IT
- Do not download or use unauthorized tools, browser extensions, or applications
- Web-based tools that handle student data must be approved by IT to ensure they meet privacy requirements

Personal Electronic Devices

- **Students** are not permitted to use, have visible, or have easily accessible any personal electronic device during the school day (8:15 AM until buses leave)
- **Staff** may only use personal devices during unassigned time — personal devices must not be visible during instructional time or in areas where students are present
- Social media platforms are restricted on school networks and devices
- Medical exemptions (e.g., glucose monitoring) require a doctor's letter submitted to the Associate Superintendent of Operations

Cybersecurity Training

- All staff are required to **periodically complete cybersecurity awareness training** and participate in phishing tests (delivered through KnowBe4)
- This helps stay informed about emerging threats and prevent cyberattacks

Network and Internet

- Do not attempt to bypass network filters or security controls
- Only FVSD-owned devices may connect to the internal network — personal devices may only connect to the guest/isolated network
- Report any network or security concerns to IT

FVSD Equipment

- Take care of FVSD devices assigned to you
- Report lost, stolen, or damaged equipment to IT immediately
- Return all FVSD equipment when you leave the division or change roles

Questions?

If you have questions about the Acceptable Use Policy or whether a specific use is appropriate, contact IT:

- **Submit a ticket** through the IT helpdesk
- **Email:** helpdesk@fvsd.ab.ca

Revision #1

Created 2026-08-06 22:44:02 UTC by Admin

Updated 2026-08-06 22:44:02 UTC by Admin