Table of Contents

Purpose 2

Responsibilities 2

Definitions 2

Account Credentials and Access Privileges 4

School Owned Devices 4

Personally Owned Devices 4

Software 5

Cloud Hosted Services 5

Network Usage 7

Wireless 7

Online Communications 7

E-Mail Communications 8

Social Media 8

Data Privacy and Protection 9

Network Monitoring and Filtering 10

Copyright 10

Technology Training 10

Reporting Incidents 11

Consequences of Breach of Procedure 11

Limitations of Liability 11

Modification and Revision 12

Purpose

The Frontier Regional/Union#38 Schools operate and manage digital resources to meet educational and operational requirements. To protect the confidentiality, integrity and availability of the enterprise network and systems, these procedures formalize the procurement and responsible use of such systems. These procedures apply to all individual students, employees, consultants, contractors and temporaries ("users") that utilize Frontier Regional/Union#38 Schools network services or devices. These procedures apply to all on-site and cloud hosted systems that utilize and rely on the enterprise Internet Protocol (IP) network.

Responsibilities

All users must sign the online consent form and demonstrate an understanding of the procedure.

Definitions

- **Devices** includes district owned/leased, employee owned devices, and student owned devices.
- **Educational Use** is defined as classroom activities, career and professional development, and high quality self-discovery activities of an educational nature.
- **Harmful to Minors** is defined as any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- **Inappropriate Material** is defined as material containing profane, harassing, obscene or sexually explicit as well as material viewed as creating a hostile workplace.
- **Information Systems** is defined as digital systems that provide Frontier Regional/Union#38 Schools work process efficiencies via database and software technologies.
- **Network and Internet services** includes Frontier Regional/Union#38 Schools wired and wireless network and Internet.
- **Personally Identifiable Information** - As defined by the state of Massachusetts, the first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:
    - Social Security number;
    - driver's license number or state-issued identification card number;
    - financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit

access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public;

  - Student ID Number to include either Local Assigned Student identification Number or State Assigned Student Identification Number
  - Massachusetts Education Personal Identification Number

- **User** includes anyone, including employees, students, contractors, consultants, temporaries and guests, using any device that accesses Frontier Regional/Union#38 Schools network and information systems.

Account Credentials and Access Privileges

Users are individually accountable for all actions under their credentials. At all times, users must keep their account passwords confidential and not share or display passwords to anyone else. Users are highly advised to sign out of services when not in use. Frontier Regional/Union#38 Schools and Office of Information Technology (OIT) staff will never ask for a user's account password for any purpose. Users are advised to report any suspicious requests for account information directly to the OIT staff.

Each user is granted specific network and system access privileges based on roles and responsibilities. Under no circumstances will users attempt to access accounts, information or systems that are not expressly authorized to them.

All official job functions must use school provided user accounts. Personal accounts, personal software or personal services must not be used to communicate, store or perform any business related tasks.

School Owned Devices

For the purpose of functionality, security and standardization, OIT must review and approve all hardware prior to purchasing. In addition to approved hardware, personal and guest devices are authorized.

All users must treat all technology equipment with the utmost care and respect.

Students must not remove school devices from the school premises. School devices must be appropriately secured within the school when not in use. Exceptions to this rule requires a written agreement with families. Employees may take devices outside the school so long as they maintain employment with the organization.

Additional security measures may be necessary to protect any sensitive data stored on the devices. Such instances may include but limited to, denying access to critical systems with personal or non school-owned devices.

Personally Owned Devices

Employee personal devices are allowed to access a designated wireless network at any time. During school hours, students may only use personal devices on the school network with the permission of designated school administrators and the OIT staff. The Director of Technology reserves the right to suspend access if an imminent risk to the school network exists.

During the school hours, visitors are required to obtain wireless credentials to access the network. After school hours, the school and community members may access the guest wireless network.

Personal devices brought onto school property are subject to searching and system scanning for malicious software or other problems. All users must keep their personal devices up to date with a minimum of malware protection and operating system updates. OIT Staff reserve the right to deny access until the device meets the minimum security requirements.

At any time, OIT Staff may determine a need to further limit or change the use of personal devices due to security concerns.

Software and Digital Resources

Installation of software (commercial, shareware, or freeware) of any type on school devices must be approved by OIT staff. All device software must be approved in accordance with the software request procedures listed below.

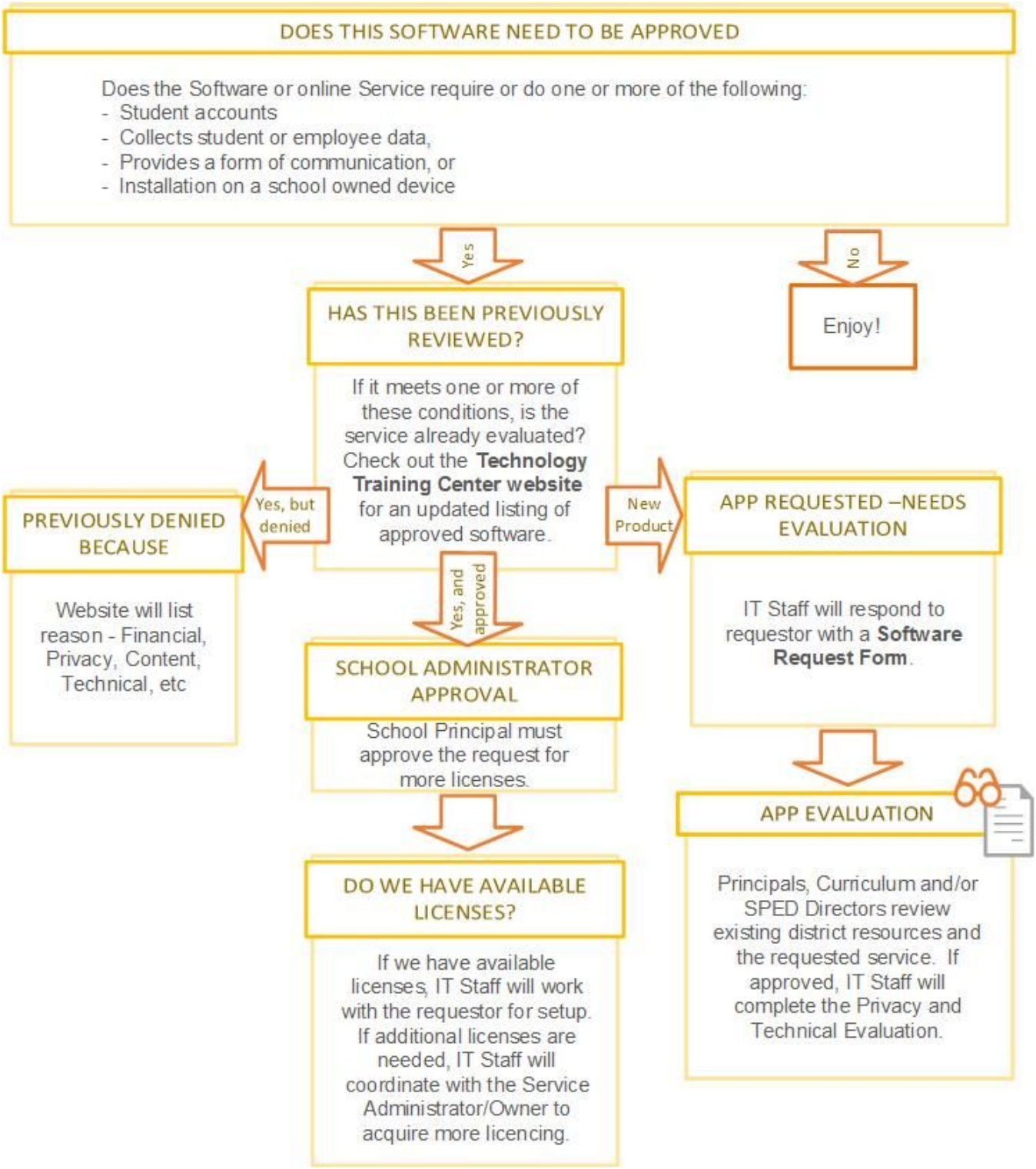
OIT does not support the acquisition of software and digital resources for personal devices.

Cloud Hosted Software and Digital Resources

If a digital resource is provided via a cloud hosted platform, such as Software as a Service, and requires one or more of the following:

1. Student accounts,
2. Collects student or employee data,
3. Provides a form of communication, or
4. Installation on a school owned device,

users are required to follow the same software approval process before the service is used for academic or operational purposes. The following flowchart is designed to streamline the process as much as possible. By reviewing these products, school administrators can ensure the product is curriculum focused, technically sound and meets legal data privacy requirements.


DOES THIS SOFTWARE NEED TO BE APPROVED
Does the Software or online Service require or do one or more of the following:
- Student accounts
- Collects student or employee data,
- Provides a form of communication, or
- Installation on a school owned device
Yes
No
Enjoy!
HAS THIS BEEN PREVIOUSLY REVIEWED?
If it meets one or more of these conditions, is the service already evaluated? Check out the Technology Training Center website for an updated listing of approved software.
Yes, but denied
PREVIOUSLY DENIED BECAUSE
Website will list reason - Financial, Privacy, Content, Technical, etc
New Product
APP REQUESTED –NEEDS EVALUATION
IT Staff will respond to requestor with a Software Request Form.
Yes, and approved
SCHOOL ADMINISTRATOR APPROVAL
School Principal must approve the request for more licenses.
DO WE HAVE AVAILABLE LICENSES?
If we have available licenses, IT Staff will work with the requestor for setup. If additional licenses are needed, IT Staff will coordinate with the Service Administrator/Owner to acquire more licencing.
APP EVALUATION
Principals, Curriculum and/or SPED Directors review existing district resources and the requested service. If approved, IT Staff will complete the Privacy and Technical Evaluation.

Network Usage

Network resources and connectivity are provided for academic and operational use only. Frontier Regional/Union#38 Schools reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic or operational services.

Users must refrain from inappropriate use of the network including but not limited to;

- transmitting offensive or harassing messages; sending messages or posting comments to bully or harass a person or group;
- viewing, transmitting or downloading pornographic materials or materials that encourage others to violate the law;
- uses that cause harm to others or damage to their property;
- uploading malicious or other harmful form of programming or vandalism;
  participating in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems;
- using the network in such a way that would degrade the performance of system resources or disrupt the use of the network by others; or
- attaching unauthorized equipment to the district network without permission from the school administration or OIT staff.

Wireless

There are multiple wireless networks available in the schools that each serve a purpose. Please contact the Office of Technology if you have any questions about wireless access for visitors or personal devices.

Online Communications

Users must conduct themselves in ways that do not distract from or disrupt the educational process. Proper online decorum includes, but is not limited to, the following:

- Users must use only approved communications platforms for all official business. The list of approve platforms will be available upon request from the IT Department.
- Improper fraternization with students using social media or other electronic means.
    - Users may not friend or follow current students on social media.

- Team, class, or student organization pages, accounts, or groups will be created only in conjunction with the adult employee. All groups must include the appropriate administrator as a member. Access to the page will remain with the employee.
- All contact and messages by employees with team members shall be sent to all team members, except for messages concerning medical or academic privacy matters, in which case the messages will be copied to the appropriate administrator.
- Users will not give out their private cell phone or home phone numbers without prior approval of the Principal.

- Inappropriate contact via phone or electronic device is prohibited.
- Inappropriateness of posting items with sexual content
- Inappropriateness of posting items exhibiting or advocating the use of drugs and alcohol
- Examples of inappropriate behavior from other districts, as behavior to avoid

E-Mail Communications

When conducting official school business or instruction, users must use school provided email addresses and online services approved by the district. All users are encouraged to separate personal and school communication activity. Use of a personal e-mail accounts or communication tools to conduct school business may be subject to investigations. All proper etiquette for online communications apply to e-mails. Under no circumstances will school e-mail systems be used to foster commercial interests or individual interests. Unless encryption technology is applied, e-mail communication is considered an insecure communication and therefore shall not be used to communicate Personally Identifiable Information or sensitive data such as Social Security Numbers.

Social Media

This procedure establishes guidelines for the creation and use of social media sites for work related purposes as a means of conveying information to the public. For purposes of this procedure, "Social Media" is understood to be content created by individuals, using accessible, expandable and upgradable publishing technologies, through and on the Internet. For purposes of this procedure, "Content" includes comment, information, articles, pictures, videos or any other form of communicative content posted on Frontier Regional/Union#38 Schools' Social Media sites.

The establishment and use of social media sites must be approved via the software and services approval procedure. The Frontier Regional/Union#38 Schools will approach the use of social media tools as consistently as possible across all school districts.

Social Media sites shall be administered and monitored by employees jointly approved by the principals and the Superintendent or designee. Site administrators must follow the school's media release policy and procedures.

Social media sites should make clear that they are maintained by the Frontier Regional/Union#38 Schools and that they follow the Social Media Policy.

All Frontier Regional/Union#38 Schools' Social Media sites shall adhere to applicable federal, state and local laws, rules, regulations and policies. Frontier Regional/Union#38 Schools' Social Media sites are subject to Massachusetts public records and record retention laws, rules, regulations and policies. Any content maintained in a Social Media format that is related to Frontier Regional/Union#38 Schools' business, including a list of subscribers, posted communication, and communication submitted for posting, may be a public record subject to public disclosure. The department site administrator will maintain records in accordance with Massachusetts public records and record retention laws, rules, regulations and policies.

The Frontier Regional/Union#38 Schools' website at www.frsu38.org/ will remain the Frontier Regional/Union#38 Schools' primary and predominant Internet presence. The primary websites should link to the social media sites. Wherever possible, Frontier Regional/Union#38 Schools' Social Media sites should link back to the official Frontier Regional/Union#38 Schools' website.

Comments or other content on topics or issues not related to Frontier Regional/Union#38 Schools' business or within the jurisdictional purview of the Frontier Regional/Union#38 Schools may be removed.

Content perceived as inappropriate is subject to removal and/or restriction by site administrators, the Superintendent of Schools, or their designees

Employees representing the Frontier Regional/Union#38 Schools via Frontier Regional/Union#38 Schools' Social Media sites shall conduct themselves at all times as representatives of the Frontier Regional/Union#38 Schools in accordance with all Frontier Regional/Union#38 Schools' rules, regulations and policies.

Data Privacy and Protection

Access to view, edit, or share personal data on students and employees maintained by employees, or by persons acting for the district must abide by local, state, and federal laws and regulations, such as the Family Educational Rights and Privacy Act.

Student and employee information may only be shared with individuals deemed eligible to have authorization and access by the person(s) responsible for oversight of that data. Outside parties and/or non-Frontier Regional/Union#38 Schools individuals requesting protected data must follow school procedures to request access.

Network Monitoring and Filtering

Frontier Regional/Union#38 Schools OIT staff monitor the use of the school network to protect the integrity and operation of all devices, information systems and networks. OIT staff employs the use of systems that monitor and record all network activity. At the request of the Frontier Regional/Union#38 School Districts school administrators, Frontier Regional/Union#38 School administrators reserve the right to monitor, inspect, copy, review, and store all communications, data and usage information of technology devices, digital resources, and network infrastructure to substantiate inappropriate activity, troubleshoot technology issues and to comply with requests of law enforcement agencies. There is no expectation of privacy regarding such information regardless if it is personal in nature or not.

For Information Security reasons and the Children's Internet Protection Act (CIPA), Frontier Regional/Union#38 Schools utilizes internet content filtering technology to prevent access to inappropriate content or content that poses a risk to the confidentiality, integrity, and availability of the network. The filtering mechanisms will be applied to school devices both on and off campus. Designated school employees will also monitor the online activities of students through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is deemed inappropriate or harmful to minors.

Copyright

Violations of copyright law that occur while using the Frontier Regional/Union#38 Schools network or other resources are prohibited and have the potential to create liability for the district as well as for the individual. All users must comply with procedures on copyright plagiarism that govern the use of material accessed through the Frontier Regional/Union#38 Schools network. Users will refrain from using materials obtained online without requesting permission from the owner if the use of the material has the potential of being considered copyright infringement. Frontier Regional/Union#38 Schools will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network.

Technology Training

There are several technology related training events and training options that are made available to users. Due to state mandated information security programs and organizational best practices, all users are annually required to partake in a security awareness training. In addition, the Office of Technology staff provide professional development trainings, self-paced training modules and individual assistance. Please contact the Office of Technology for more information.

Reporting Incidents

Users are required to report misuse or breach of policies or procedures to appropriate personnel, including building administrators, direct supervisors and to the Office of Information Technology (OIT) staff. Users should also report any suspicious activity or situation that is a potential threat to users, devices, systems or other technology related services.

Consequences of Breach of Procedure

Use of all Frontier Regional/Union#38 Schools technology resources is a privilege, not a right. By using Frontier Regional/Union#38 Schools Network Systems and devices, the user agrees to follow all Frontier Regional/Union#38 Schools policies, procedures and guidelines. District and technology administration reserves the right to examine, use and disclose any data found on the district network and or equipment in order to further the health, safety, discipline or security of the school community. Abuse of these privileges may result in one or more of the following consequences:

- Suspension or cancellation of use or access privileges as determined by the administrator.
- Payments for damages or repairs.
- Discipline under appropriate School Department policies, up to and including termination of employment.
- Liability under applicable civil or criminal laws.

Limitations of Liability

Frontier Regional/Union#38 Schools and its' employees and agents, make no warranties of any kind, either expressed or implied, concerning the network, Internet access, and electronic resources it is providing. All users shall assume full liability, legal, financial or otherwise, for their actions while connected to the internet. Furthermore, the districts are not responsible for:

- the accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access;
- any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices;
- unauthorized financial obligations resulting from the use of Frontier Regional/Union#38 Schools electronic resources; or
- inappropriate or offensive material students encountered on the Internet.

Parents/guardians should discuss the Technology Use Responsibilities with their children. Questions and concerns can be forwarded to the Frontier Regional/Union#38 Schools and appropriate offices. Parents

and guardians agree to accept financial responsibility for any expenses or damages incurred as a result their student's inappropriate or illegal activities on the Frontier Regional/Union#38 Schools network.

Modification and Revision

The Frontier Regional/Union#38 School Administration reserves the right to modify or change this procedure and related implementation procedures at any time.

Revision	Date	Approver	Notes
1.0	6/30/2019		