SAU 70 Student Acceptable Use Policy

Purpose
SAU 70 is fortunate to provide its students a variety of technological resources to enhance learning and support communication with others. The District's technological resources allow students to participate in real time global events, collaborate with others, and extend learning outcomes beyond traditional outcomes.

The District intends to offer these opportunities within an environment that fosters safe, legal, ethical, and responsible use. The guidelines outlined in this policy apply to use of District equipment, networks, and resources on and off school property, and extends to privately owned devices that are used in conjunction with school systems. This policy governs both students and guest users on the use of school Network resources.

This policy also serves to meet or exceed Federal, State, and local laws and regulations as related to student technology use in SAU 70.

Definitions
The term "Network" shall be interpreted to include any and all District owned computers, servers, any hardware or software, the District's local area network (LAN), all wireless access points, the Internet, the District Intranet, self-contained electronic mail systems, and any other elements of the District's computer, telecommunications or electronic communication/information systems.

Regulation
Regulation of the SAU 70 Acceptable Use Policy is the responsibility of the building Technology Coordinators, the SAU Superintendent or his/her designee in conjunction with the individual school administrators. This body reserves the right to prohibit conduct, communication, or content which it deems harmful to individual users, to the school community, to the network itself, or illegal activity. In addition, this body may impose consequences for violations of the acceptable use policy based on the guidelines listed.

Expectations
Students of SAU 70 are expected to abide by the guidelines delineated below:

Use of Computers, Chromebooks, and Mobile Devices
Computers, Chromebooks, iPads and all other devices at SAU 70 are for educational purposes. It is within a teacher's purview to limit the use of such devices to support our educational goals. SAU 70 employs the use of third-party applications to regulate and monitor technological resources for violations of this AUP as well as to protect and maintain a safe environment for learning. SAU 70 filters content in accordance with Federal law that has been categorized as bullying, pornographic, obscene, illegal, terroristic, profane, or harassing. Content filters are managed by the District Technology Director and can be manipulated to accommodate instructional goals as needed at each individual school.

Social Media
Social media refers to online tools and services that allow any Internet user to create and publish content. Many of these sites use personal profiles where users post information about themselves. Social media allows those with common interests to share content easily, expanding the reach of their ideas and work.

While social networking is a valuable tool for connecting and communicating outside the classroom, there are some risks to consider when using these tools.

Below are guidelines to follow when representing SAU 70 on social media platforms.

Always:

- Maintain a secure and private password
- Be respectful. Represent yourself and your school positively and be considerate of others' opinions.
- Be ethical. Never publish or share private information about yourself or others.
- Assume all content, whether personal or school-related, is public.
- Be accurate and appropriate in posts. Utilize spelling and grammar check. If mistakes are made, correct them and take responsibility for any errors.
- Notify a teacher or administrator if any social media action may impact others' well-being or safety.
- Never create or knowingly share or engage with falsified accounts. Advocate for those who may have been victims of falsified accounts and report this information to an administrator.
- Refrain from publishing images, audio, or video of an individual or group without consent.
- Refrain from representing an official school organization, class, or sport without permission from a coach, teacher, or administrator.

At no time, should students be asked to use personal social media accounts to log on to required applications, or modify social media privacy settings in order to access required content.

Use of Email, Chat, and Other Electronic Communications
SAU 70 supports multiple resources for electronic communication. When grade level appropriate, students are expected to use these applications to communicate with teachers and classmates and for networking purposes related to higher education. When grade level appropriate, it is the student's responsibility to regularly check email for schoolwide communications. School email is considered public record. Students are strongly discouraged from using non-school resources for communicating with school personnel.

Internet Access
The Internet offers vast, diverse, and unique resources. Student use of the Internet is closely linked to the mission and goals of the school. SAU 70 firmly believes that the value of the information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is inconsistent with the educational goals of the district. SAU 70 educates students in the responsible, safe, and ethical use of the

Internet. Users should adhere to the following safety and behavior guidelines in order to protect the school's ability to provide this resource to the community.

The use of the school's network and Internet resources should support the educational objectives of the school. Access to the Internet is a privilege and not a right. Users should take responsibility for their own behavior. Inappropriate behavior may result in the loss of this privilege. Technology is constantly changing and because of that fact, the guidelines for Internet use, listed below are also subject to change.

Safety
In the interest of protecting personal safety, users should be cautious with giving out personal information and should take steps to understand about "secure" communications.

Users should avoid:

- transmitting personal information such as full name, driver's license number, financial data, home and/or cell phone number. sending content that is lewd, suggestive, or that involves nudity, clicking on the links or downloading anything sent from unknown people or links or messages that are out of character for people you do know.
- using non-school resources for school communications (ie. social media, texting)

Behavior
Users are expected to be polite and considerate of other users, to use appropriate language in electronic communications, and to confine their use of computing resources to further educational objectives.

The following behaviors are considered unacceptable:

- Damaging devices and their peripherals. This includes removal or alteration of peripherals, identifying labels, barcodes, or serial numbers.
- Using information technology resources for commercial purposes, partisan political purposes, or for any unlawful purpose.
- Using electronic media to harass or threaten other persons, or to display, design, copy, store, draw, print, or publish obscene language or graphics.
- Repeatedly or purposefully engaging in activities which unreasonably tax computing and network resources or go beyond their intended or acceptable use. Borrowing, lending, falsifying or misusing a computer account, or allowing, or facilitating the unauthorized access to use of school computing resources by a third party.
- Using school computing resources to gain or attempt to gain unauthorized access to computing resources either inside or outside of school.
- Interfering with the operation of the school's information technology resources by deliberately attempting to degrade or disrupt resource performance, security, or administrative operations.
- Intercepting or attempting to intercept or otherwise monitor any communications not explicitly intended for him or her without authorization.
- Copying, reading, accessing, using, misappropriating, altering, publishing or destroying computer files, output data, documents or other files of another individual or attempts to do so, without the permission of that individual, teacher, or authorized administrator.

- Making, distributing and/or using unauthorized duplicates of copyrighted material, including software applications, proprietary data, and information technology resources. This includes sharing of entertainment (e.g., music, movies, video games) files in violation of copyright law.
- Violating the terms and conditions of software license agreements for software distributed by the school, by giving, lending, selling, or leasing such media or software to others for their own use.
- Using school resources to access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/ or illegal materials, images (still or video), messages, and text.
- Excessive use of resources for personal affairs (shopping, gaming, streaming media, etc.)
- Using electronic communications in any manner which violates school/District policies or local/state/Federal laws.

Privacy
Users of SAU 70 network resources acknowledge that all technology provided by SAU 70 is actively monitored and **should not be considered private**, regardless of the location of the device. Accessing content which indicates harm to self or others, illegal activity, and unethical and unsafe behavior will be communicated to building administration and/or their designee.

Beginning in the 2019-2020 school year, all digital resources provided to or recommended to students will be vetted for compliance with NH and/or VT student data privacy regulations. Students who create accounts or exercise Single Sign On options using SAU 70 resources independently assume all responsibility for the sharing of their own personal data.

Consequence
Consequences for abuse of technology and/or network resources by students at SAU 70 may include but not be limited to schedule up, suspension of technology or network use, suspension from school or in some cases legal action as deemed necessary by the local school administrator(s) in cooperation with the local school Technology Coordinator(s) and the District Technology Director.