INFORMATION TECHNOLOGY PROGRAM REGULATION

Acceptable Use Policy (AUP)

The Saranac Central School District ("District") places a high value on digital citizenship, as well as promoting personal accountability when using digital resources provided by the District. The District provides its student, faculty, and staff access to a variety of technology resources. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. The District intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. "District Technology" in this policy means all hardware, software, online services, cloud services, devices, wired and wireless networks, access to the Internet, and technology and uses not yet available. Employees, students, and other users of District Technology and resources agree to follow this policy when using technology provided by the District. This policy applies to all users of District Technology including but not limited to students, faculty, staff, and other users unless specifically noted. Individual users of the District Technology are responsible for their behavior and communications when using those resources. Responsible use of the District Technology is use that is ethical, respectful, academically honest and supportive of student learning. All users of the District Technology, including independent users off premises, shall be subject to this policy and other related District policies.

I. Purpose:

A. The District Technology is provided to support the educational mission of the school. Internet access, electronic mail (e-mail), hardware, software and network resources are available to faculty, staff, and students in the Saranac Central School District solely for educational and instructional purposes and other purposes consistent with the educational mission of the District.

B. The District Technology was not established as a public access service and the District has placed appropriate restrictions on the material users may access or post through the District Technology.

II. User Access

A. Students, substitutes, non-district personnel, and guest users must have a valid Acceptable Use Access Agreement to be permitted authorized use of the District Technology. Users will be issued a network username and password. Use of the District Technology without authorization is strictly prohibited.

B. A valid Student Acceptable Use Access Agreement requires signature by the student (grades 3-12) and his/her parent or guardian and approved by the District. Student Acceptable Use Access Agreements may be terminated by a student and/or his/her parent or guardian upon written notice to the District. Student Acceptable Use Access Agreements may also be terminated by the District at any time for violation of the District's policy or regulations.

C. All network users will be issued a login name and password. Passwords must be changed periodically. If you suspect your password has been compromised in any way, your password will need to be changed. For password changes, follow appropriate procedures.

D. By using the District Technology, users have agreed to this policy.

E. The Acceptable Use Access Agreement does not attempt to articulate all required and/or acceptable uses of the District Technology nor is it the intention of this policy to define all inappropriate usage. All users shall adhere to the laws, policies and rules governing District Technology including but not limited to copyright laws, rights of software publishers, license agreements, Children's Internet Protection Act (CIPA), Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA).

F. Student access to District Technology shall terminate upon graduation or withdrawal from the District. Employee access to District Technology shall terminate upon separation of employment from the District.

G. Any District owned laptop and/or any other District owned device(s) must be returned immediately upon leaving the District.

III. <u>Responsible Use</u>

A. Access to the District Technology is provided for educational purpose consistent with the District's mission and goals.

B. District Technology users have the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette.

C. All network users are responsible for proper use of their account and must take all reasonable precautions to prevent others from being able to use their account. Under no circumstances should users provide their password to another person.

D. Any network users identifying a security problem must notify the appropriate teacher, administrator or the technology department.

E. Respecting Resources

i. Users of email will check their email frequently, deleting unwanted messages promptly.

ii. Keep your District provided electronic storage space cleaned of unnecessary files.

iii. Users will only print when necessary to conserve resources (toner, ink, paper, etc).

iv. Conserve the District's consumables.

IV. <u>Unacceptable Use</u> of the District Technology by users includes but is not limited to:

A. Attempting or gaining unauthorized access to the District Technology, including networks, computers, and informational systems is prohibited;

B. Attempting or gaining unauthorized access to any other computer system through use of the District Technology is prohibited;

C. Attempting or exceeding authorized access to the District Technology including, but not limited to, attempting to log in through another person's account or accessing another person's files is prohibited;

D. Providing access or disclosing user(s) username or password to an unauthorized person is prohibited;

E. Attaching unauthorized devices to the District network;

F. Any attempt to circumvent or disable the filter or any security measure is prohibited;

G. Attempting to disrupt or disrupting the District Technology including, but not limited to, damaging equipment, destroying data, hacking, cracking, vandalizing, malware, ransomware, viruses, and changes to hardware, software, and monitoring tools is strictly prohibited;

H. Downloading, installing and use of unauthorized materials or applications without permission or approval from the Technology Department is prohibited;

I. Accessing or use of material or language which is considered obscene, profane, lewd, vulgar, rude, inflammatory, violent, threatening or disrespectful, as determined by the District, is prohibited on the District Technology. Action constituting harassment, intimidation, or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes, and remarks is prohibited. This may also include the manufacture, distribution, or possession of inappropriate digital images;

J. Accessing, uploading, downloading, storage or distribution of obscene, pornographic, or sexually explicit materials is prohibited;

K. Engaging in any unlawful use of the District Technology is strictly prohibited;

L. Posting, sending, and/or storing material that present a potential for damage, danger and/or disruption to the District Technology is prohibited;

M. Refusal or failure to follow the direction from another person or organization to stop sending messages is prohibited;

N. Reposting a message sent privately without permission of the original sender is prohibited;

O. Posting private information about another person is prohibited;

P. Posting chain letters or sending annoying or unnecessary messages, including but not limited to spam is prohibited;

Q. Reproduction of material protected by copyright without authorization is prohibited;

R. Unauthorized actions that result in liability or cost incurred by the District is prohibited;

S. Personal gain, commercial solicitation, and compensation of any kind is prohibited with District Technology;

T. Use of the District Technology for political lobbying is prohibited.

V. Student Safety

A. Students will not provide personal contact information about themselves or others including, but not limited to, home address, telephone number or school address.

B. Students will not agree to meet with anyone introduced online without the consent of the student's parent or guardian. Students should be accompanied by a parent or guardian to any such meeting.

C. Students will promptly disclose to teachers or other school employees any message received that is inappropriate or makes them feel uncomfortable.

VI. Security and Privacy

A. Security

i. Filtering software is used to block or filter access to inappropriate content, including visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Users must take responsibility for use of the District Technology and avoid objectionable sites.

ii. Passwords are the first level of security for a user account. User accounts are to be used only by the authorized owner of the account. Safeguard all of your credentials.

iii. Lock or log off if leaving the computer.

iv. Student/employee data is confidential. District staff must maintain the confidentiality of student data in accordance with District policies, Family Educational Rights and Privacy Act (FERPA), and Children's Online Privacy Protection Act (COPPA). Any suspected data breach must be immediately reported to a supervisor, administrator or the technology department.

B. Privacy

The District shall have both the authority and the right to review or monitor, with or without prior notice, the content of electronic communication for any reason, including but not limited to retrieval of information, investigation or resolution of network or communications problems, prevention of system misuse, ensuring compliance with policies for use of third-party software and information, ensuring compliance with legal and regulatory requests and enforcement of all District policies. The District also reserves the right to review, inspect the content of, and monitor all information residing on all computers and file servers for such purposes. District Technology users waive any right to privacy in anything they create, store, send, or disseminate on the District's computers and computer network systems, including the Internet.

VII. Consequences of Inappropriate Use

Any violation of this policy may result in withdrawal of the privilege of the use of the District Technology or in restricted use of it, and may result in disciplinary action and/or legal action.

VIII. Limitations of Liability

A. The District makes no guarantee that the functions or the services provided by or through the District Technology will be error-free or without defect. The District is not responsible for the accuracy or quality of the information obtained through or stored on the District Technology and will not be responsible for any damage, including but not limited to, loss of data or interruption of service experienced.

B. The District will not be responsible for any financial obligation arising through unauthorized use of the District Technology.

C. The District will cooperate fully with local, state, or federal officials in any investigation related to any alleged unlawful activities conducted through the District Technology.

Adoption Date: March 5, 2013

Revised Date: December 3, 2018