9101: Rules and Protocols for the Responsible Use of Technology Resources and Instruction Policy

PURPOSE:
This Rules and Protocols for the Responsible Use of Technology Resources and Instruction Policy # 9101 is set forth in support of Responsible Use of Technology Resources and Instruction Policy # 9100 and serves the purpose of identifying certain, but not all, of those actions and/or activities which are considered by the Scituate School Department (herein after referred to as SSD) to be responsible uses of technology. The primary purpose of the SSD computer-based communications network is to support research, education, and communication by providing access to unique resources and an opportunity for collaborative work. Each individual's activity on the network must be in support of these objectives.

The Scituate School Committee believes that technology offers vast, diverse, and unique resources to both students and staff. Our goal is to promote educational excellence in our schools and to graduate responsible digital citizens. The SSD will advance academic achievement and 21st century skills by purposefully aligning pedagogy with use of technology and by facilitating innovation and communication.

REGULATIONS:

1. All SSD network users and users of SSD supplied computers or electronic devices are held accountable to the Responsible Use of Technology Agreement. All students and parents will sign, or electronically sign, the Responsible Use of Technology Agreement. The signature(s) on the agreements is (are) legally binding and indicates the party (parties)who signed has (have) read the terms and conditions carefully and understand(s) its significance. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards children should follow when using these resources. It is our expectation that students will access the Internet only as directed by SSD staff. Parents/guardians are expected to discuss these policies with their child. In regards to staff, it is the School Committee's expectation that the resources be used foremost and primarily for school-business purposes.

2. Any activity, which is in violation of federal or state law, or SSD policy, or disruptive to the normal operation of the SSD instructional process, the Responsible Use of Technology Resources and Instruction Policy # 9100, or the Internet Filtering Policy # 9102 will be considered unacceptable and subject to sanctions.

3. Sanctions are listed, but not limited to the following:
   a. Violation(s) of any of the above policy or rules may result in loss of access.
   b. Additional disciplinary action may be determined by the school staff in accordance with existing SSD policies, procedures, rules, and regulations, including financial restitution.
   c. When applicable, law enforcement agencies will be notified and involved.

9101: Rules and Protocols for the Responsible Use of Technology Resources and Instruction Policy

GUIDELINES

1. The use of the SSD computers is a privilege which may be revoked at any time for inappropriate conduct. Such conduct includes, but is not limited to, the placing of unlawful or disruptive information on or through the computer network and the use of obscene, abusive, pornographic, or otherwise objectionable language or images in either public or private files or messages. The administration of each school will be the sole arbiter of what constitutes disruptive information as well as obscene or objectionable language or images.
2. All users must behave in a legal and ethical manner at all times. Users agree to adhere to all federal copyright rules. Any costs, liability, or damages caused by the way the user chooses to use his or her network access is the sole responsibility of the computer user.
3. Each school in the SSD reserves the right to add to or to change network guidelines for safety or educational reasons without notice.
4. The computers and the computer services owned by the SSD and SSD provided email accounts are intended for educational use of its patrons, and any commercial or other unauthorized use of those services and materials, in any form, is expressly forbidden.
5. Computer users are responsible to protect passwords by not sharing them, posting them in conspicuous places or making them obvious. The Information Technology Department will determine appropriate password change procedures and frequency.
6. Users are responsible for ensuring that the storage of confidential information on electronic devices is limited, and for ensuring the physical and electronic security of confidential information provided to or created by them.
7. The Internet Filtering Policy # 9102 is being enforced, which includes measures to block or filter Internet access for both minors and adults to certain visual depictions including obscene, pornographic, or materials that are harmful to minors with respect to use of computers with Internet access.
8. Penalties for inappropriate computer use and/or the damage of the SSD's computers and computer network will be strictly enforced including, but not limited to, financial restitution, and any other actions or restrictions as deemed appropriate by the SSD.
9. Note that electronic mail (email) is not guaranteed to be private: People who operate the SSD network do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
10. The SSD makes no warranties (expressed or implied) with respect to network services or the content of any device or information received from the School Department network.
11. The SSD permits personal use of the network and internet so long as it occurs on personal time, does not interfere with SSD activities, and is not otherwise prohibited by established policies and procedures.

9101: Rules and Protocols for the Responsible Use of Technology Resources and Instruction Policy

PROHIBITED USES

The following activities are unacceptable and are strictly forbidden at any time during the use of SSD property:

a. Misusing copyrighted materials, software, sound recordings, or images.
b. Harassment or bullying of any sort (harassment as defined by established SSD policy, local, state, and federal law).
c. Use of the network and computers to distribute hate mail, discriminatory remarks, and offensive or inflammatory communication and/or materials including but not limited to slurs, epithets, images, or anything that could be reasonably construed as offensive, objectionable, harassment or disparagement to others.
d. Committing plagiarism.
e. Accessing sexually explicit or objectionable materials.
f. Disseminating destructive/disruptive material.
g. Advertising, political lobbying, or other commercial activities unless approved by school administration.
h. Violating the privacy of other users.
i. Using the school or district name when unauthorized.
j. Soliciting without authorization.
k. Distributing unauthorized personal information such as name, address, and telephone numbers of any students or staff.
l. Damaging computer equipment, software, or network data.
m. Using obscene or inappropriate language, messages, or pictures in any format.
n. Wasting or inappropriate use of limited resources.
o. Impersonating other individuals during communication.
p. Attempting to capture or break encryption or passwords or attempting to access any system or data to which the user is not authorized to access.
q. Destroying or altering data or programs belonging to others.
r. Accessing Internet sites that contain the promotion of criminal activity, gambling, or hate speech.

Adopted 8/15/2019

Erika A. McCormick
Chairperson

8/15/2019
Approval Date