SOUTH BURLINGTON SCHOOL DISTRICT
POLICY F14

RESPONSIBLE USE OF INFORMATION TECHNOLOGY

Purpose

The South Burlington School District uses information technology resources including the Internet to support and enrich the curriculum, to allow students to benefit from access to electronic information resources and opportunities for collaboration that are uniquely provided by certain electronic technologies, and to enhance learning.

This policy is intended to ensure compliance with the requirements of applicable federal and state laws that regulate the provision of access to the Internet and other information technology resources by school districts.

Definitions. As used in this policy, the following terms shall be defined in accord with federal and, where the context clearly allows, state law.

1) **Child Pornography** means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
    a. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
    b. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
    c. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
2) **Harmful to minors** means any picture, image, graphic image file, or other visual depiction that:
    a. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
    b. 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 lewd exhibition of the genitals; and
    c. Taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.
3) **Technology protection measure** means a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.
4) **Minor** means an individual who has not attained the age of 18.
5) **Computer** means any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.
6) **Access to Internet** means a computer that is equipped with a modem or is connected to a computer network that has access to the Internet.

7) **Obscene** means materials/pictures considered offensive to accepted standards of decency or modesty.

Policy

All students and staff will use information technology resources and the Internet as fundamental learning tools. Parents who want to limit their child(ren)'s access to these resources shall contact the school principal in writing if they wish to restrict their child's access to District electronic resources, including the Internet.

The availability of access to electronic information does not imply endorsement by the District of the content, nor does the District guarantee the appropriateness or accuracy of information received. The District shall not be responsible for any information that may be lost, damaged, or unavailable when using the network.

The use by students, staff, or others of District information technology resources is a privilege, not a right. The District's computer and network resources are the property of the District. Users shall have no expectation of privacy in anything they create, store, send, receive, or display on or over the District's computer or network resources, including personal files. The District reserves the right to monitor, track, and log use of information technology resources and may deny access for unauthorized, inappropriate, or illegal activity. The District may revoke access privileges and/or administer appropriate disciplinary action for misuse of its information technology resources. The District shall cooperate to the extent legally required with local, state, and federal officials in any investigation concerning or related to the misuse of the District's Internet, computers or network.

The District shall work to ensure Internet safety for minors by taking steps that include monitoring the online activities of minors and the operation of technology protection measures with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors.

In addition to those stated in law and defined in this policy, the District deems the following to be examples of inappropriate actions by minors:

- Capturing, emailing, or publishing nude images
- Defamation of character
- Lewd, vulgar, or profane communication
- Threatening, bullying, harassing, or discriminatory behavior
- Terrorism
- Gambling

Administrative Responsibilities

The superintendent or his or her designee shall coordinate and oversee the use of District information technology resources including the Internet, and will develop procedures necessary to implement this policy. In addition, the superintendent or his or her designee shall ensure that the District, as part of its policy implementation, will educate minors about appropriate online communication which includes cyber bullying and social networking.

Administrative procedures developed under this policy shall include provisions designed to protect student data and any other confidential information stored in District information technology resources.

In addition, the administrative procedures developed under this policy shall include Internet safety measures that provide for the monitoring of online activities by minors and address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using District electronic communications.
3. Prevention of unauthorized online access by minors, including “hacking” and other unlawful activities.
4. Unauthorized disclosure, use, and/or dissemination of personal information regarding minors.
5. Restriction of minors’ access to materials harmful to them.

The administrative procedures developed under this policy shall also provide that authorized individuals may temporarily disable the District’s technology protection measures to enable access for bona fide research or other lawful purpose.

The superintendent or his or her designee shall conduct periodic analyses of the implementation of this policy, and shall make recommendations to the board as needed to ensure that the District’s approach to Internet safety is effective.

User Responsibilities

During instructional time, information technology resources including the Internet are primarily for school-related purposes. The term “school-related purposes” includes use of the system for classroom activities, such as email communication, curriculum-driven research, or career development, and other school activities.
Students and staff may access the District’s information technology resources for limited personal use. Limited personal use of the District’s information technology resources including the Internet may be allowed if the use:

- imposes no tangible cost to the District;
- does not unduly burden the District’s information technology resources;

- occurs during non-instructional time and does not impede other student or staff access for educational purposes;
- does not adversely impact student learning and/or staff responsibilities; and
- does not violate this policy.

Students will not post personal contact information about themselves or other people and are required to follow administrative safety procedures when using electronic communications, including the Internet.

All users of District information technology resources are expected to act in a responsible, ethical, and legal manner. Specifically, the following uses are prohibited:

1. Commercial or for-profit uses.
2. Commercial product advertisement or political lobbying.
3. Bullying or harassment
4. Offensive or inflammatory communication, including profanity, hate mail, discriminatory remarks, or "sexting."
5. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
6. Accessing sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic, lewd, or otherwise illegal materials, images, or photographs.
7. Impersonation of another user.
8. Loading or using unauthorized games, programs, files, or other electronic media.
9. Disabling or bypassing the Internet blocking/filtering software without authorization.
10. Accessing, sending, receiving, transferring, viewing, sharing, or downloading confidential information without authorization.

Parental Notification and Responsibility

Each school will provide annual notice to parents/guardians about student responsible use of District information technology resources including the Internet, the policies and procedures governing their use, and the limitation of liability of the District. The annual notice shall direct parents/guardians to contact the school principal in writing if they wish to restrict their child's access to District electronic resources, including the Internet.

Limitation/Disclaimer of Liability

The District is not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, or costs incurred by users. The District is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the District's information technology resources network including the Internet. The District is not responsible for any damage experienced, including, but not limited to, loss of data or interruptions of service. The District is not responsible for

the accuracy or quality of information obtained through or stored on the information technology resources system including the Internet, or for financial obligations arising through their unauthorized use.

Enforcement

In the event there is an allegation that a user has violated this policy, a student will be provided with notice and opportunity to be heard in the manner set forth in the student disciplinary policy.

Allegations of staff member violations of this policy will be processed in accord with contractual agreements and legal requirements.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to illegal activities conducted through the use of the District's information technology resources including the Internet.

POLICY
Date Policy Warned: October 5, 2011
Date Policy Considered: November 2, 2011
Date Policy Adopted: November 2, 2011

Signed:

Richard T. Cassidy, Chair
Elizabeth E. Fitzgerald, Clerk
Martin J. LaLonde
Julie H. Beatty
Diane M. Bugbee

AUTHORITY AND CROSS REFERENCE

Legal References

17 U.S.C. §§101-120 (Federal Copyright Act of 1976 as amended)

20 U.S.C. § 6777 et seq. (Enhancing Education Through Technology Act)

18 U.S.C. §2251 (Federal Child Pornography Law—Sexual Exploitation and Other Abuse of Children)

47 U.S.C. §254 (Children's Internet Protection Act)
47 CFR §54.520 (CIPA Certifications)

13 V.S.A. §§2802 et seq. (Obscenity, minors)
13 V.S.A. § 1027 (Disturbing Peace by Use of…Electronic Means)
13 V.S.A. §2605(Voyeurism)

Cross References

Student Conduct and Discipline (F1)

Copyrights (G2)

Selection of Instructional Materials (G5)

Complaints About Instructional Materials (G6)