09/17/2013

ACCEPTABLE USE POLICY AND PROCEDURES

CODE G
(Mandatory)[1]

Orange Windsor Supervisory Union

3590 VT Route 14
South Royalton, Vermont 05068

Purpose

The Orange Windsor Supervisory Union (OWSU) Board of School Directors supports the use of electronic resources including the Internet to implement 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 staff professional development.

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 electronic resources by school districts.

Policy

Access to District electronic resources including the Internet will be available to students and staff who agree to abide by the requirements of this policy. User agreements, except as otherwise described in this policy, will be required prior to allowing any individual unsupervised access to OWSU electronic resources.

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

---

[1] The federal No Child Left Behind Act (NCLBA) makes schools ineligible to receive funding for the purchase of computers used to access the internet, or to pay costs associated with accessing the internet, through the technology grants program "...unless the school, school board, local educational agency, or other authority with responsibility for administration of (the) school both...has in place a policy of Internet safety for minors that includes the operation of a technology protection measure 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; and is enforcing the operation of such computers by minors; and has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are...obscene or child pornography and is enforcing...such measure during use of any such computers..." 20 U.S.C. § 6777; 47 U.S.C. § 254(h)(5)(A) & (B). Prior to adoption, the school must "provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy." 47 U.S.C. § 254(l)(1)(B).

The use of district electronic resources by students, staff, or others is a privilege, not a right. The district's computer and network resources, hardware, software, and infrastructure 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 computers or network resources, including personal files. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action for misuse of its electronic 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 Superintendent or his or her designee shall coordinate and oversee the use of District electronic resources including the Internet, and will develop procedures necessary to implement this policy.

Definitions.

As used in this policy and its procedures, 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 create, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.[2]
2) **Harmful to minors** means any picture, image, video (multi-sensory frame), graphic image file, movies, or other visual/auditory 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]

[2] 18 U.S.C. § 2256. See, 13 V.S.A. § 2801(6) for the state definition of this term. Federal law requires the use of the federal definition in this policy.

[3] Federal law defines "minor" as a person who has not yet attained the age of 17. 20 U.S.C. § 6777; 47 U.S.C. § 254. Vermont's anti-obscenity law defines the term "minor" as "any person less than 18 years old." 13 V.S.A. § 2801(1). The Vermont definition is used in this model policy as it includes the federal requirement and also provides coverage for students until they reach the age of 18.

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]
4) **Minor** means an individual who has not attained the age of 18.[5]
5) **Computer** means any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.[6]
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]

[4] 47 U.S.C. § 254
[5] See footnote 3 above.
[6] 20 U.S.C. § 6777(e)(1)
[7] 20 U.S.C. § 6777(e)(2)

Procedures:

The district shall operate technology protection measures during the use of any of its computers with Internet access, including those computers not accessible to minors, that protect against access through such computers to material inappropriate for minors, including but not limited to, visual depictions that are obscene or child pornography.[8]

In addition, the Superintendent or his or her designee shall ensure that the district, as part of its implementation of this policy, is educating minors about appropriate on-line behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.[9] Educational efforts will include instruction in Internet safety for minors including 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.[10]

The following materials, in addition to those stated in law and defined in this policy, are inappropriate for access by minors:

- Defamatory
- Lewd, vulgar, or profane
- Threatening
- Harassing or discriminatory
- Bullying
- Terroristic
- Disruptive to the educational process to school operations or any school activity

Administrative procedures developed under this policy shall include provisions necessary to ensure that Internet service providers and other contractors comply with applicable restrictions on the collection and disclosure of student data and any other confidential information stored in District electronic 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[11] and address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

[8] 20 U.S.C. § 6777(a)(2)(A); 47 U.S.C. § 254
[9] Required by 47 U.S.C. § 254(h)(5)(B)
[10] 47 U.S.C. § 254(h)(B)
[11] Required by 47 U.S,C. § 254(h); 47 C.F.R. § 54.520(C)(i)

2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, dissemination of personal information regarding minors.
5. Restriction of minors' access to materials harmful to them.[12]

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.[13]

The Superintendent or his or her designee shall conduct an annual analysis 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 school hours, users may access electronic resources including the Internet for school related purposes only. The term "school related purpose" includes use of the system for classroom activities, which may involve e-mail communication, career development, and curriculum driven research. It also includes use of the system for other school activities such as sports, other co-curricular activities and school sponsored fund raising activities.

The District may provide e-mail access for students and staff. Students and staff may use real-time electronic communication, such as chat or instant messaging only for specifically organized educational activities.

Students will not post personal contact information about themselves or other people and agree to follow communication safety requirements outlined in administrative procedures when using electronic communications including the Internet.

All users of District electronic resources are expected to act in a responsible, ethical and legal manner. Specifically, the following uses are prohibited:[14]

1. Commercial or for-profit uses.
2. Product advertisement or political lobbying.
3. Bullying or harassment[15]
4. Offensive or inflammatory communication, including hate mail, discriminatory remarks or "sexting."[16]

---

[12] Required by 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)

[13] Required by 20 U.S.C. § 6777(c)

[14] This list of prohibited uses is not specifically required by federal or state law. It is suggestive, and can be modified by boards that adopt acceptable use policies.

[15] 13 V.S.A. § 1027 makes it a crime in Vermont to "disturb peace by use of telephone or other electronic communications." Actionable activities under the statute include threatening, harassing, intimidating communications as well as the use of "obscene, lewd, lascivious or indecent language" with intent to harass or intimidate by telephone or other electronic communication.

[16] 13 V.S.A. § 2802b makes activities commonly referred to as "sexting" by minors illegal in Vermont.

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. Inappropriate language or profanity.[17]
8. Impersonation of another user.
9. Loading or using unauthorized games, programs, files or other electronic media.
10. Disabling or bypassing the Internet blocking/filtering software without authorization.
11. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

Students and staff may access the District's electronic resources for limited personal use. Limited personal use of the District's electronic resources including the Internet shall be allowed if permission is granted by the superintendent or his or her designee in advance, and the use:

- imposes no tangible cost to the District;
- does not unduly burden the District's electronic resources;
- occurs during non-instructional time and does not impede other student or staff access for educational purposes; and
- does not violate this policy.[18]

Parental Notification and Responsibility

Each school will provide written annual notice to parents/guardians about student use of District electronic resources including the Internet, the policies and procedures governing their use, and the limitation of liability of the District. Parents/guardians must sign an agreement to allow their child(ren) to access District electronic resources including the Internet and return this agreement to the school before access will be granted. Students18 years of age or older must sign their own agreement. A signed user agreement will not be required when students are using school computers for research as part of a course requirement and the use is supervised by a responsible adult.[19]

Limitation/Disclaimer of Liability

The District is not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, and 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 electronic 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 electronic resources system including the Internet, or for financial obligations arising through their unauthorized use.

---

[17] 13 V.S.A. § 2605 makes "voyeurism" illegal in Vermont.

[18] This section on Limited Personal Use is not a required component of this policy, and is therefore an option for consideration by boards adopting acceptable use policies.

[19] As an alternative to requiring signed user agreements, a district could provide clear notice that it will allow access to its electronic resources unless notified in writing by parents that they do not consent to such use by their children.

Enforcement

In the event there is an allegation that a student 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 electronic resources including the Internet.[20]

---

[1] The federal No Child Left Behind Act (NCLBA) makes schools ineligible to receive funding for the purchase of computers used to access the internet, or to pay costs associated with accessing the internet, through the technology grants program "...unless the school, school board, local educational agency, or other authority with responsibility for administration of (the) school both...has in place a policy of Internet safety for minors that includes the operation of a technology protection measure 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; and is enforcing the operation of such computers by minors; and has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are...obscene or child pornography and is enforcing...such measure during use of any such computers..." 20 U.S.C. § 6777; 47 U.S.C. § 254(h)(5)(A) & (B). Prior to adoption, the school must "provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy." 47 U.S.C. § 254(l)(1)(B).

[2] 18 U.S.C. § 2256. See, 13 V.S.A. § 2801(6) for the state definition of this term. Federal law requires the use of the federal definition in this policy.

[3] Federal law defines "minor" as a person who has not yet attained the age of 17. 20 U.S.C. § 6777; 47 U.S.C. § 254. Vermont's anti-obscenity law defines the term "minor" as "any person less than 18 years old." 13 V.S.A. § 2801(1). The Vermont definition is used in this model policy as it includes the federal requirement and also provides coverage for students until they reach the age of 18.

[4] 47 U.S.C. § 254

[5] See footnote 3 above.

[6] 20 U.S.C. § 6777(e)(1)

[7] 20 U.S.C. § 6777(e)(2)

[8] 47 U.S.C. § 254(h)(B)

[9] *Neighborhood Children's Internet Protection Act,* 47 U.S.C §254(l)(2); 47 C.F.R. 54.520. *See also, Children's Internet Protection Act,* 47 U.S.C. § 254. These federal statutes require that "(A) determination what matter is inappropriate for minors shall be made by the school board (or) local education agency..."

[10] 20 U.S.C. § 6777(a)(2)(A); 47 U.S.C. § 254

[11] Required by 47 U.S.C. § 254(h)(5)(B)

[12] Required by 47 U.S,C. § 254(h); 47 C.F.R. § 54.520(C)(i)

[13] Required by 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)

[14] Required by 20 U.S.C. § 6777(c)

[15] This list of prohibited uses is not specifically required by federal or state law. It is suggestive, and can be modified by boards that adopt acceptable use policies.

[16] 13 V.S.A. § 1027 makes it a crime in Vermont to "disturb peace by use of telephone or other electronic communications." Actionable activities under the statute include threatening, harassing, intimidating

communications as well as the use of "obscene, lewd, lascivious or indecent language" with intent to harass or intimidate by telephone or other electronic communication.

[17] 13 V.S.A. § 2802b makes activities commonly referred to as "sexting" by minors illegal in Vermont.

[18] 13 V.S.A. § 2605 makes "voyeurism" illegal in Vermont.

[19] This section on Limited Personal Use is not a required component of this policy, and is therefore an option for consideration by boards adopting acceptable use policies.

[20] As an alternative to requiring signed user agreements, a district could provide clear notice that it will allow access to its electronic resources unless notified in writing by parents that they do not consent to such use by their children.

[21] See 13 V.S.A. §§ 2802b and 1027 for examples of criminal activities involving electronic resources.

Date Warned:

Date Adopted:

Legal Reference(s):

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 Reference:

Student Conduct and Discipline (F1)

Copyrights (G2)

Selection of Instructional Materials (G5)

Complaints About Instructional Materials (G6)

Personal Devices, Bring Your Own Device (BYOD) at South Royalton School

Philosophy:

The South Royalton School believes that electronic devices are valuable resources to support and enrich the curriculum and school community. The benefits of these devices outweigh the potential disadvantages for students. It is the philosophy of the South Royalton School to teach and model responsible device and resource use in a developmentally appropriate manner. The school feels that acceptable use of technology lies in behavior, not technology, however care should be taken that technology is not used to the detriment of face-to-face social interaction.

Parameters of Use:

Beginning in grade 6, all students with grades of "C" or above may possess and use personal, electronic, and digital devices at the following times:

- before and after school
- during lunch
- in study hall (with teacher's permission)
- between classes (grades 9-12 only)

During classes, such devices may be used as appropriate tools when so directed by the teacher or with the teacher's permission.

Privilege of Use:

By default, students automatically have the privilege to possess and use personal devices as outlined above. The loss of this privilege can result from neglecting intellectual, social, or emotional responsibilities.

Intellectual Responsibility:

- Any quarterly or semester grades below a "C"

Social/Emotional Responsibility:

- Unacceptable effort level in class
- Unacceptable behavior during the school day
- Use of personal devices to proliferate bullying or harassing behaviors
- Use of personal devices in an inappropriate manner, to include, but **not limited to**:
  - Taking photos without permission
  - Copying academic material/plagiarizing
  - Playing offensive music, videos, or games
  - Viewing inappropriate content
  - Using other students' devices without permission
  - All other behaviors included in OWSU District policy above

Loss of this privilege and its duration, based on the above criteria, will be determined by a team that may include a teacher or teachers, the planning room coordinator, an administrator, and the school IT faculty member. Loss of privilege due to a violation of the student's social/emotional responsibilities, as stated above, will be handled through the school's current disciplinary protocol. The cause and duration of loss of privileges as a result of disciplinary action will be clearly stated in the discipline notice. Loss of privilege due to quarterly or semester grades below a "C" will require that the student prove to the team that his/her grades are in the "C" or above range in order to regain the privilege.

Loss of the privilege will result in a mandatory surrender of all personal devices at the start of the school day. During a loss of privilege, the team may determine that students be permitted to access school-owned devices, for academic purposes only, during any class period (with the exclusion of study hall and lunch) under direct supervision of a teacher or paraprofessional. Students caught with personal devices while on restriction may face further disciplinary action (detention / suspension).

Assumption of Risk:
Students who choose to bring their own device to school do so at their own risk. The school does not take responsibility for lost or damaged items. Students are encouraged to safeguard their devices at all times.

The School reserves the right to inspect devices (school owned or personal) upon suspicion of misuse or abuse. Students have no expectation of privacy for their personal devices once they bring them on campus or use them in any way connected with other students or the school itself. Devices may be confiscated, searched, or turned over to proper authorities (with subpoena).

Parent/Guardian Permission
Student Name (please print): _____

Parent/Guardian Name (please print):_____

Date: _____

Parent/Guardian Signature: _____

Student Permission
I have read, understand and agree to abide by the "Acceptable Use Policy and Procedures." I further understand that any violation of the Procedures as outlined above may enact school disciplinary action or constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary actions may be taken, and/or appropriate legal action may be initiated.

Student's Name (please print):_____

Student Signature: _____

Date:_____

Staff Agreement on Use of Technology as per the Acceptable Use Policy and Procedures

Name (Printed)_____

Signature _____

Date _____

cc: central personnel file, school personnel file