

**WINOOSKI SCHOOL DISTRICT  
POLICY ON RESPONSIBLE USE OF TECHNOLOGY**

**Purpose**

The Winooski Board of School Trustees recognizes that information technology (IT) is integral to learning and educating today's children for success in the global community and fully supports the access of these electronic resources by students and staff.

The purpose of this policy is to:

1. Create an environment that fosters the use of information technology in a manner that supports and enriches the curriculum, provides opportunities for collaboration, and enhances staff professional development.
2. Ensure the district takes appropriate measures to maintain the safety of everyone that accesses the district's information technology devices, network and web resources.
3. Comply 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**

It is the policy of the Winooski School District to provide students and staff access to a multitude of information technology (IT) resources including the Internet. These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond. However, with the privilege of access comes the responsibility of students, teachers, staff and the public to exercise responsible use of these resources. The use by students, staff or others of district IT resources is a privilege, not a right.

The same rules and expectations govern student use of IT resources as apply to other student conduct and communications, including but not limited to the district's harassment and bullying policies.

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 computers or network resources, including personal files and electronic communications.

The superintendent is responsible for establishing procedures governing use of IT resources consistent with the provisions of this policy. These procedures must include:

1. An annual process for educating students about responsible digital citizenship. As defined in this policy, a responsible digital citizen is one who:
  - **Respects One's Self.** Users will maintain appropriate standards of language and behavior when sharing information and images on social networking websites and elsewhere online. Users refrain from distributing personally identifiable information about themselves and others.
  - **Respects Others.** Users refrain from using technologies to bully, tease or harass other people. Users will report incidents of cyber bullying and

harassment in accordance with the district's policies on bullying and harassment. Users will also refrain from using another person's system account or password or from presenting themselves as another person.

- **Protects One's Self and Others.** Users protect themselves and others by reporting abuse and not forwarding inappropriate materials and communications. They are responsible at all times for the proper use of their account by not sharing their system account password.
  - **Respects Intellectual Property.** Users suitably cite any and all use of websites, books, media, etc.
  - **Protects Intellectual Property.** Users request to use the software and media others produce.
2. 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.
  3. Technology protection measures that provide for the monitoring and filtering of online activities by all users of district IT, including measures that protect against access to content that is obscene, child pornography, or harmful to minors.
  4. Methods to address the following:
    - Control of access by minors to sites on the Internet that include inappropriate content, such as content that is:
      - ✓ Lewd, vulgar, or profane
      - ✓ Threatening
      - ✓ Harassing or discriminatory
      - ✓ Bullying
      - ✓ Terroristic
      - ✓ Obscene or pornographic
    - The safety and security of minors when using electronic mail, social media sites, and other forms of direct electronic communications.
    - Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
    - Unauthorized disclosure, use, dissemination of personal information regarding minors.
    - Restriction of minors' access to materials harmful to them.
  5. A process whereby authorized persons may temporarily disable the district's Internet filtering measures during use by an adult to enable access for bona fide research or other lawful purpose.

### **Policy Application**

This policy applies to anyone who accesses the district's network, collaboration and communication tools, and/or student information systems either on-site or via a remote location, and anyone who uses the district's IT devices either on or off-site.

**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.

**Enforcement**

The district reserves the right to revoke access privileges and/or administer appropriate disciplinary action for misuse of its IT resources. In the event there is an allegation that a user has violated this policy, the school district will handle the allegation consistent with the student disciplinary policy.

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

1st Reading: April 11, 2018

2<sup>nd</sup> Reading: May 9, 2018

Approved by Board of School Trustees: May 9, 2018

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(s): WSD Policy #5114 (a): Student Conduct and Discipline

## **PROCEDURES:**

The use of the technology shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students.

The district's electronic network is part of the curriculum and is not a public forum for general use. All use of the district's electronic network must be:

- (1) In support of education and/or research, and be in support of the Winooski Board of Trustees policy statement.
- (2) For a legitimate business purpose.

Use is a privilege, not a right. General rules for behavior and communications apply when using technology. All users shall employ appropriate ethics and protocols. The District's Authorization for Technology Access contains the appropriate uses, ethics, and protocol.

Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school administrators or designees.

The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

All students, employees and School Board members shall be subject to this policy.

## **ADMINISTRATIVE PROCEDURE** **ACCEPTABLE USE OF TECHNOLOGY**

All use of technology shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

### **Terms and Conditions:**

1. **Acceptable Use** - Access to the district's technology electronic networks must be (a) for the purpose of education or research, and be consistent with the educational objectives of the district, or (b) for legitimate business use.
2. **Privileges** - The use of the district's technology and electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges.

3. **Unacceptable Use** - The user is responsible for his or her actions and activities involving the district's technology and electronic network. Some examples of unacceptable uses are:
- a) Using the district's technology and electronic network for any illegal activity, including violation of copyright or other contracts or transmitting any material in violation of any U.S. or state law;
  - b) Unauthorized downloading of software, regardless of whether it is copyrighted or de-  
virused;
  - c) Downloading copyrighted material for other than personal use;
  - d) Using technology for private financial or commercial gain;
  - e) Wastefully using resources, such as file space;
  - f) Gaining unauthorized access to resources or entities;
  - g) Using another user's account or password;
  - i) Posting material authorized or created by another without his/her consent;
  - j) Posting anonymous messages;
  - k) Using technology for commercial or private advertising;
  - l) Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
  - m) Using technology while access privileges are suspended or revoked.
4. **Network Etiquette** - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
- a) Be polite. Do not become abusive in messages to others.
  - b) Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
  - c) Do not reveal the personal addresses or telephone numbers of students or colleagues.
  - d) Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
  - e) Do not use technology in any way that would disrupt its use by other users.

f) Consider all communications and information accessible via technology to be private property.

5. **Disclaimer of Liability** - The school district shall not be liable for students' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The school district shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

The school district makes no guarantee that the functions or the services provided by or through the school district system will be error-free or without defect. The school district will not be responsible for any damage a user may suffer, including but not limited to, loss of data or interruptions of service. The school district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The school district will not be responsible for financial obligations arising through the unauthorized use of the system.

6. **Filtering** - Filtering is used in conjunction with other strategies to selectively restrict access to clearly objectionable and educationally inappropriate content; e.g. pornographic sites, non-educational chat rooms. If filtering is used as part of a school's procedures, filtering must provide for limited and flexible restriction of Internet sites. Decisions regarding the use of filtering technology must take into account the age and developmental levels of the students. The filtering must allow for selective decision-making by designated school officials.
7. **Indemnification** - The user agrees to indemnify the school district for any losses, costs, or damages, including reasonable attorney fees, incurred by the district relating to, or arising out of, any violation of these procedures.
8. **Security** - Network security is a high priority. If the user can identify a security problem on the Internet, the user must immediately notify the building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Any user identified as a security risk may be denied access to the network.
9. **Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
10. **Telephone Charges** - The district assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.
11. **Copyright Web Publishing Rules** - Copyright law prohibit the re-publishing of text or graphics found on the Web or on district web sites or file servers without explicit written permission.

- a) For each re-publication (on a web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
- b) Copyrighted material must not intentionally be downloaded from any system connected to the network without the author's permission. Copyrighted material may be downloaded and used for educational purposes, but the source must be cited and all copyright laws applied.
- c) The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- d) Student work may only be published with permission from the parent, Technology Coordinator or designee.

**12. Use of Electronic Mail:**

- a) The district's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the school district. The school district provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
- b) The district reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- c) Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter of memorandum.
- d) Electronic messages transmitted via the school district's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the school district. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this school district. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- e) Any message received from an unknown sender via the Internet should be immediately deleted. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- f) Use of the school district's electronic mail system constitutes consent to these regulations.

- g) Computer viruses must not knowingly be spread. Each school will take appropriate measures to protect local workstations and servers from propagating computer viruses.