CODE: D3

RESPONSIBLE COMPUTER, NETWORK & INTERNET USE

Purpose

The Slate Valley Unified Union School District 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 Supervisory Union 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 Slate Valley Unified Union 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[1] 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.

[1] For the purposes of this policy, "personally identifiable information" shall not include any information listed as "directory information" in the school district's annual FERPA notice.

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.[2]
4. Methods to address the following:[3]
    - 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.[4]

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.

[2] Required by Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)
[3] Required by Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)
[4] Required by 20 U.S.C. § 6777(c)

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, 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.

Date Warned: *February 21, 2018*
Date Adopted: *March 12, 2018*
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)

Slate Valley Unified Union School District

RESPONSIBLE COMPUTER, NETWORK & INTERNET USE PROCEDURE

The superintendent is responsible for establishing procedures governing use of IT resources consistent with the provisions of the Responsible Computer, Network & Internet Use policy to include the following.

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 Supervisory Union'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.

Procedure
Students in grades K-8 will receive education through library classes at each school, along with occasional school-wide assemblies. Students in grades 9-12 have student led assemblies where topics centered around responsible digital citizenship are discussed. Throughout the year they also work on public service announcements (PSA) through different school groups. This will be coordinated by the District Director of Operations with each school reporting annually to the District Director of Operations as to the completion of these trainings.

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 Supervisory Union electronic resources.

Procedure
The district reviews Internet service and other technology contracts with vendors to ensure that the vendor adheres to the Family Educational Rights and Privacy Act (FERPA) and other as applicable. All technology contracts are to be reviewed by the District Director of Operations before being authorized.

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.

Procedure
The district deploys content filtering systems on our network that filter as required by the Children's Internet Protection Act (CIPA). These systems allow for the review of websites accessed. The content filtering system is overseen by the District Director of Operations and supported at the school level by technology staff.

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.

Procedure
The district deploys content filtering systems on our network, which is overseen by the District Director of Operations and supported at the school level by technology staff that filter access from minors to the website categories listed above and others as deemed inappropriate. Student email is randomly audited to assure compliance to policy by school level technology staff. Annually, staff signs a confidentiality agreement regarding student information in accordance with the Family Educational Rights and Privacy Act (FERPA). Students in grades 9-12 are required to logon with their network credentials to access social media sites, whereas students in grades K-8 are currently blocked from accessing social media sites.

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.

Procedure
Staff accounts have the ability to logon with their network credentials to access websites beyond those that are available in the default filtering policy. With prior approval from the Superintendent and/or the District Director of Operations technology staff may completely disable the content filtering system to investigate violations of the Responsible Computer, Network & Internet Use. For allegations that require working in conjunction with law enforcement the Superintendent and/or District Director of Operations shall be the point of contact for the duration of the investigation.

* **These procedures may change as deemed necessary by the Superintendent**.