ACCEPTABLE USE OF DISTRICT INTERNET/TECHNOLOGY RESOURCES-STAFF

Policy 522.7

Computer technology is used to enhance learning and support instruction for all staff. Computer networks allow individuals to interact electronically with other people within a school building and within the District. The Internet allows individuals to interact electronically with people and networks throughout the world. It is the policy of the School District of Slinger that all computer technology shall not be deemed private and shall be used in a responsible, efficient, ethical, and legal manner. School computers and Internet access is for educational purposes. Failure to adhere to this policy is a violation of school rules and shall result in the immediate revocation of access privileges. Additional disciplinary action up to and including dismissal and referral to legal authorities may result. Unacceptable uses of school district computer technology by staff include, but are not limited to:

1. Violating any district policy or state or federal law;
2. Accessing, creating, transmitting, or retransmitting inappropriate items including pornographic material, materials using profanity, obscenity, or other language and images which offend community standards or which promotes violence or advocates destruction of property;
3. Communicating with students via non-district approved applications/devices for non-school related purposes, including, but not limited to, use of social networking sites, personal e-mail accounts, instant messaging, forums, text messaging, etc. Contact with students without any clear educational purpose is prohibited, unless there is a family or other legitimate relationship justifying the amount and nature of the contact.
4. Accepting or linking students as "friends" on personal internet sites such as Facebook or other similar sites.
5. Copying software, music, artwork, etc. in violation of copyright laws. Internet materials used in class should be completely previewed and correctly cited following the same procedures as referenced printed materials;
6. Using technology for personal financial gain, commercial venture, or illegal activity;
7. Damaging or destroying any component of technology, including hardware, peripherals, or files;
8. Malicious use of any technology, including hardware, peripherals, or files;
9. Posting anonymous, discriminatory, harassing or threatening messages;

10. Using encryption software, hacking, using unauthorized packages, from any point of access within the school district;
11. Using, copying, or modifying another person's logins, passwords, files, or personal information. Users shall not give their passwords to any other user;
12. Revealing names and personal student information on the Internet;
13. Committing or attempting to commit any willful act involving the use of the network which disrupts the operation of the network within the District or any network connected to the Internet.
14. Sharing any unauthorized information or files.

The School District of Slinger does not condone the use of offensive material. Therefore, the District uses an Internet filter to block inappropriate sites and to a lesser degree high-risk activities. However, the District cannot control all of the content or the validity of the information available from the Internet. Filtering is not infallible. The District is not responsible for advice offered over the Internet. The District is not responsible for materials accessed on the Internet by any user and is not responsible for the effect that information has on the user. To help ensure staff safety while using the Internet, the district has software in place that monitors and records Internet use and will report suspicious activity to appropriate administration.

Selection and use of technology resources by staff shall be aligned with school curriculum. Staff supervision is required when students are in the labs or using technology resources, including teacher-approved chat sites and wikis.

Staff are responsible at all times for the proper use of any technology accounts and are responsible for their behavior and communication on the Internet. Staff members must use generally accepted rules of network etiquette including appropriate language. Personal computers may not be connected to the District's network without specific permission from the Director of Technology or Network Administrator.

The District reserves the right to review any electronic messages, transmissions, or files at its discretion. The use of passwords does not guarantee confidentiality and the District maintains the right to access information on the school network in spite of a password. The District email system provides a method of communication and information storage for district employees. Messages stored on the district's computers remain

district property for which employees have no expectation of privacy. These messages will not be automatically deleted and will be stored and maintained by the District in accordance with applicable maintenance laws, district policy, and rules.

Employees shall not electronically record by audio, video, or other means, any conversations or meetings unless each and every person present has been notified and consents to being electronically recorded. Persons wishing to record a meeting must obtain consent from anyone arriving late to any such meeting. Employees shall not electronically record telephone conversations unless all persons participating in the telephone conversation have consented to be electronically recorded. These provisions are not intended to limit or restrict electronic recording of publicly posted Board meetings, grievance hearings, or any other Board sanctioned meeting recorded in accordance with Board policy. These provisions are not intended to limit or restrict electronic recordings involving authorized investigations conducted by District personnel, or authorized agents of the District, or electronic recordings that are authorized by the District, e.g. surveillance videos, extracurricular activities, voicemail recordings.

Legal References:

Wisconsin Statutes

Sections 19.31 – 19.37 [Wisconsin Public Records Law]	
Sections 19.62 – 19.80	[Personal Information Practices]
Section 120.12(1)	[School Board Duty; care, control and management of school district property]
Section 120.44(2	[School Board Duties and Powers]
Section 943.70	[Computer crimes]
Section 947.0125	[Unlawful use of computerized communication systems]

Wisconsin Administrative Code

ADM 12	[Electronic records management]

Federal Laws

Children's Internet Protection Act (CIPPA	Internet safety policy
Title 17 U.S.C.	[Use and copying of copyrighted materials, including "fair use"]
18 U.S.C. Subsection 2510-22	[Electronic Communications Privacy Act]

Cross References:

Adoption Date: *6/24/2019*