Purpose

The Two Rivers Supervisory Union School Districts recognize that information technology (IT) is integral to learning and educating today's children for success in the global community and fully support 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 districts take appropriate measures to maintain the safety of everyone that accesses the districts' 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.[1]

Policy

It is the policy of the Two Rivers Supervisory Union School Districts 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 districts' harassment and bullying policies.

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

a. **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.
b. **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 districts' 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.
c. **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.
d. **Respects Intellectual Property.** Users suitably cite any and all use of websites, books, media, etc.
e. **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. Procedures to address the following:
   a. Control of access by minors to sites on the Internet that include inappropriate content, such as content that is:
      - ✓ Obscene
      - ✓ Threatening
      - ✓ Harassing or discriminatory
      - ✓ Bullying
      - ✓ Terroristic
      - ✓ Child exploitative materials
   b. The safety and security of minors when using electronic mail, social media sites, and other forms of direct electronic communications.
   c. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
   d. Unauthorized disclosure, use, dissemination of personal information regarding minors.
   e. Restriction of minors' access to materials harmful to them.
   f. Subject to approval by authorized persons may temporarily disable the district's Internet filtering measures max be disabled for 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 districts' network, collaboration, and communication tools, and/or student information systems either on-site or via a remote location, and anyone who uses the districts' IT devices either on or off-site.

Limitation/Disclaimer of Liability

The districts are not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, and costs incurred by users. The districts is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the districts' electronic resources network including the Internet. The districts are not responsible for any damage experienced, including, but not limited to, loss of data or interruptions of service. The districts are 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. The duties imposed on the district by this policy do not operate to make the district vicariously or directly responsible for the conduct of its users which violate this policy, or any of the general code of conduct of other policies.

Enforcement

The districts reserve the right to revoke access privileges and/or administer appropriate disciplinary action for misuse of its IT resources. including for any conduct which separately violates the Prevention of Harassment, Hazing and Bullying Policy, or other code of conduct or District policies, and for anyone using another person's system account or password or presenting themselves as another person.

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.

District/Board:	Replaces Policy	Review Only	First Read	Date Warned	Date Adopted
Two Rivers Supervisory Union			04/04/2024	04/19/2024	05/02/2024
Green Mountain Unified School District			04/18/2024	05/06/2024	05/16/2024
Ludlow-Mount Holly Unified Union School District			04/02/2024	04/28/2024	05/08/2024