STAFF ACCEPTABLE USE OF INFORMATION TECHNOLOGY AND COMMUNICATIONS RESOURCES

The Richfield School District is committed to supporting a safe environment that allows students to learn while using 21st Century skills. Technology resources are provided to enhance and support all teaching and learning. Additionally, the District supports access to information and technology resources by school stakeholders (students, staff, community, parents, etc.) and strives to ensure that the use of technology is efficient, safe, and appropriate.

Privacy

Communication over email and other telecommunication networks should not be considered private. Although the District does not make a practice of monitoring individual messages or use of equipment, the District Administrator/designee is authorized to access and review such usage and reserves the right to retrieve the content for legitimate reasons, such as to find lost messages, to comply with investigations of wrongful acts, or to recover from system failure. The District Administrator /designee may also examine other communications in order to ascertain compliance with network procedures for acceptable use. Email and other telecommunication messages transmitted over District networks are considered District property and may be subject to provisions of the state public records law.

The District shall take appropriate corrective action or disciplinary action against an employee based upon information obtained from monitoring or inspecting his/her district equipment, telephone and/or electronic records and communications. The District's practice of not monitoring every communication is not a waiver of its right to monitor in the future. The District retains the right to confiscate any District-owned equipment at any time.

Communication

District staff will utilize electronic mail (e-mail) on a regular basis as a primary tool for communications. The District relies upon this medium to communicate information, and all employees will be responsible for checking and reading messages on a regular basis.

Discrimination, Harassment, Cyber-bullying

All forms of harassment through the use of technology commonly referred to as cyberbullying, are unacceptable and viewed as a violation of this policy. Cyberbullying includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings. The District's computer system may not be used to defame others or disclose sensitive personal information about others.

Internet Safety

All users are advised that access to the Internet includes the potential for access to materials that are inappropriate or harmful to minors. Staff and students must take responsibility for his or her use of the Internet and avoid sites and activities that are inappropriate or harmful to minors. Staff will provide developmentally appropriate guidance to students as they make use of technology and

communication resources. Staff will inform students of their rights and responsibilities as users of the district technology and communication resources.

To the best of its ability, it is the Richfield School District's policy to: (a) prevent access by minors to inappropriate matter on the Internet; (b) instruct in the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) prevent unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) enforce measures restricting minors' access to materials harmful to them per the Children's Internet Protection Act.

Non-District Owned Technology/Software

Use of non-district owned technology can jeopardize the district's ability to verify copyright compliance or compromise the district network systems (voice, video, or data). Permission must be obtained from Technology Services to connect any personally owned equipment to District network resources prior to use. The use of USB-based storage devices that do not require software installation are allowed (e.g. flash pens, digital cameras, etc.).

Website Publishing

The goals of the Richfield School District website are to provide an effective communication tool between the school district and students, parents, and community; to provide a teaching resource for educators; and to publish student work as a showcase for the achievements of the Richfield School District students. All material posted to the Richfield School District website must follow the guidelines of the above goals, project a positive image of the district, and preserve the confidentiality of students and staff. The following guidelines must be followed:

- All information must accurately reflect the mission, goals, policies, and curriculum of the Richfield School District
- Staff or student work that is published must relate to the curriculum or to a school activity
- Material should be accurate
- Pages must be maintained regularly
- Links to personal home pages is prohibited
- Web pages may not carry advertisements for anything other than school events or school fundraising activities
- No student photographs should be published if the parent/guardian has checked the Opt-out choice on the Student Acceptable Use Policy signature page
- Student first name plus last initial may be used, but never together with a photograph
- Student first name plus last name should not be published
- Content may not reveal home address, phone numbers, other family details, or personal information of staff or students not related to the function within the school district

The district web manager and/or District Administrator may withdraw pages that do not conform to the above guidelines.

Unacceptable Uses

Examples of behaviors **not permitted** while using district information technology and communication resources include, but are **not limited to**:

- Attempting to vandalize, disconnect or disassemble any network or computer component
- Attempting to gain unauthorized access to the District system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files, folders or documents without their permission.
- Accessing, downloading, sending, or displaying sexually explicit images and materials
- Using obscene or inappropriate language or content
- Sending messages that are offensive, defamatory, discriminatory or intended to frighten, intimidate, abuse, harass or attack another person, including cyber-bullying
- Engaging in practices that threaten the network or intentionally waste limited resources (e.g. willfully introducing a virus, downloading music or videos that may overload district server space, gambling, etc.)
- Violating copyright laws
- Assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition
- Using accounts not assigned to them
- Sharing account information with others
- Failing to reasonably protect confidential information or distributing unauthorized confidential information
- Failing to manage online academic student activities (e.g., unsupervised blog sites, wikis, forums)
- Revealing personal data of students and staff (e.g. PIN, social security number, credit card numbers, addresses, phone numbers, etc.).
- Using the system for commercial or personal gain or in such a way that violates District policy, state law, or federal law
- Personal communication via non-District sponsored applications or devices between staff and students, including but not limited to: the use of social networking sites (i.e., Facebook, MySpace), instant messaging and texting
- Excessive personal use of technology resources during work hours as determined by the District Administrator
- Engaging in other behaviors in violation of district policy, work rules or law

Responsibility for Information Obtained/Lost

The Richfield School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District does not warrant that the functions of the system will meet any specific requirements the user may have, or that it will be error-free, or that its operation will not be interrupted. The District will not be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or use time) sustained or incurred in connection with the use, operation, or inability to use the hardware. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Enforcement

All users are subject to the laws and penalties of the local, state, and federal government. Inappropriate use of the district technology may be cause for disciplinary action in accordance to the severity of the violation as deemed appropriate by the District Administrator.

Legal References

Section 118.125 Wis. Stats. Student Records
Section 943.70 Wis. Stats. Computer Crimes
Section 947.0125 Wis. Stats. Computer Harassment
PL 94-553 Federal Copyright Law
Children's Internet Protection Act (CIPA)
Children's Online Privacy Protection Act (COPPA)
Family Education Rights and Privacy Act (FERPA)

I have received, read, and understand the contents of the STAFF ACCEPTABLE USE OF INFORMATION TECHNOLOGY AND COMMUNICATIONS RESOURCES Policy. I understand that the District retains the sole discretion to add to, modify, or delete any provision, guideline, or policy, as well as to reprimand, discipline or discharge an employee for failure to adhere to District policy.

Name (Please Print) _____

Employee Signature _____

Date _____