SCHOOL DISTRICT OF SPRING VALLEY
Spring Valley WI 54767

Policy Code: **363.2 RULE**

INTERNET SAFETY AND ACCEPTABLE USE RULES

Use of the computers and technology resources at the School District of Spring Valley is a privilege not a right. Students and employees must use computers and the Internet in an acceptable manner, including when accessing the District wireless network while using one's own technology device. Failure to follow District Internet Safety and Acceptable Use policy and rules will result in disciplinary action and/or legal action as applicable. There is no expectation of privacy in any use of District technology resources. Acceptable use includes but is not limited to the following:

1. Treat computer hardware and software and all technology resources carefully and appropriately so it will continue to be available for use by students and employees.

2. Protect your password. Keep it private and secret. Never allow another person to know or use your password.

3. Respect District computer server resources. Save only what is needed. Discard files that are no longer used. Avoid clutter in your folder. Do not download software without specific approval of the Building Principal in consultation with the Technology Coordinator.

4. Ask for help if you are unsure of what to do in any computer application or with any technology resource.

5. Model proper behavior around the computers/technology. Keep the area clean, and free of food and drink.

6. Use school technology and personal devices consistent with the educational objectives of the School District of Spring Valley. Accessing or transmitting materials that are obscene, sexually explicit, pornography, or child pornography is prohibited.

7. All forms of harassment over the Internet, commonly referred to as cyber bullying, are unacceptable. Cyber bullying 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 e-mail messages, instant messages, text messages, digital pictures or images, or Web site postings, including blogs.

8. Transmission of any materials in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to, copyrighted material and threatening or obscene material. Information accessible via the Internet should be assumed to be subject to copyright protections. Use of these sources shall be credited appropriately as with the use of any copyrighted material.

9. Users shall abide by the rules of Internet etiquette. These include using appropriate language, respecting the privacy of other users, and not disrupting the use of the network by other users.

10. For their own safety, users should not reveal any personal addresses, phone numbers, or credit card numbers. Financial transactions are prohibited without specific approval of the Building Principal in consultation with the Technology Coordinator.

11. Students may not subscribe to “list servers” or “newsgroups” without prior permission of the Building Principal in consultation with the Technology Coordinator.

12. Certain Web 2.0 services such as wikis, podcasts, RSS feeds, social networking sites, and blogs that emphasize online educational collaboration and sharing among users may be permitted by the District. However, such use must be approved by the Building Principal in consultation with the Technology Coordinator. District authorized training may be required.

13. Attempts to gain unauthorized access to system programs or computer equipment are prohibited. Unauthorized access to and damage to any computer or software/hardware system may result in a financial assessment equal to the cost to repair the damage.

14. Any malicious attempt to harm, modify, or destroy data of another user is prohibited.