RIVER VALLEY SCHOOL DISTRICT

660 West Daley Street ≈ Spring Green, Wisconsin 53588 ≈ Phone: 608-588-2551

Acceptable Use of Networked Computers, Electronic Mail, and Internet Safety Policy

The RVSD computer network, because it is connected to the Internet, enables district students and staff to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The Board believes that the benefits to users from access in the form of information resources and opportunities for collaboration exceed the disadvantages.

Telecommunications, electronic information sources, and networked services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. Electronic information research skills are now fundamental to preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources without discrimination.

Students and staff shall be trained on the use of Internet Safety to include communicating with other individuals on social networking websites and chat rooms as well as cyber bullying awareness and response. Principals will be responsible for informing students and staff of the District's policies, procedures, and rules annually.

The network is provided for users to conduct research and communicate with others. Users are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. All activity through the River Valley network is subject to the right of the River Valley School District to monitor, access, read, and review.

CIPA and N-CIPA

The School District must comply with the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (N-CIPA), which protect students from prohibited material.

Prohibited Use of District Computers

The following activities are prohibited for all users of the RVSD computer network:

- Sending or displaying messages that defame, slander, or libel another person
- Sending or displaying offensive messages or pictures including, but not limited to, pornographic or erotic images or racial, sexual, or religious jokes
- Using obscene language and/or racial slurs
- Harassing, insulting, or attacking others
- Cyber bullying or cyber harassment of others
- Damaging computers, computer systems, or computer networks
- Use of or downloading unauthorized software
- Violating copyright laws
- Disclosing one's password to anyone else, or using another's password
- Trespassing in another's folder, work, or files

- Intentionally wasting limited resources and/or spending an unusual or extraordinary amount of time on personal e-mail conversation or Internet "surfing"
- Employing the network for unapproved commercial purposes
- Engaging in criminal activity
- Use of social networking sites deemed to be inappropriate
- Unauthorized access, including "hacking" and other unlawful activities
- Unauthorized disclosure, use, and dissemination of personal identification and/or confidential information (such as student records, employment records, health information)
- Any other activity inappropriate for an educational setting

Violations may result in a loss of access, as well as other disciplinary or legal action. A summary of this policy is contained in student handbooks for each building level.

Management, Administration, Monitoring, and Privacy

1. The District may at any time put software and systems in place that monitor and record all computer usage to ensure the systems are being used for educational purposes, consistent with the District's goals. The District wants users to be aware that our security systems are capable of recording, for each and every use, each World Wide Web site visit, attempts to reach World Wide Web sites, the amount of time spent actively using the World Wide Web, each chat, newsgroup access, e-mail message, and every file and/or program transfer into and out of our internal networks to the Internet, and we reserve the right to do so at any time, without advance notice or warning to the user. No District user should have any expectation of privacy as to his or her Internet usage, or the privacy or any electronic mail message, file, download, note, or other data stored on or transmitted or received through any District computing facility. The District will review computing activity and analyze usage patterns, and may choose to publicize this data to assure that the District's computing resources are devoted to maintaining the highest standards of educational benefit and employee productivity.

2. The District, through appropriate management personnel to include the district network administrator and/or members of administration, reserves the right to inspect any and all data stored in public or private areas of networked and individual storage systems of any kind, without notice or warning, and at any time or for any purpose.

3. The District uses independently supplied facilities to identify and block Internet content that is inconsistent with the educational and professional development goals of the District. We will block access from within our networks to all such sites that we know of or that our facilities identify. To be clear, these facilities endeavor to block us**e** of the network to create, view, send, receive, store, display, or print text or graphics that may reasonably be construed to be obscene, disruptive or harmful to the educational or working environment, but we acknowledge that no blocking or filtering mechanism is capable of blocking all inappropriate content all of the time. Offensive, disruptive, or harmful data include, but are not limited to any messages or files, or data that contain the following:

   - Pornographic or erotic images
   - Sexual implications, nudity
   - Racial slurs, discriminatory comments
   - Derogatory gender-specific comments and/or other inappropriate language
   - Information or instructions designed to cause physical harm to another person
   - Comments that offensively address a person's age, sexual orientation, religious beliefs, political beliefs, national original, or disability
   - Any comment which in any way defames, slanders, or libels another person
   - Any comment intended to frighten, intimidate, threaten, abuse, annoy, or harass another person

- Those data or activities that invade the privacy of another person
- Drugs, violence, crime and/or the encouragement thereof
- Auction sites that don't monitor for weapons or other sexual items or illegal items

If a user finds that he/she is connected to a site that contains any of the above material, he/she must disconnect from that site immediately, regardless of whether that site has been previously deemed acceptable by any screening or rating program, and inform the teacher or supervisor of the incident. Similarly, a user is encouraged to inform his or her supervisor if he or she becomes aware that another user is accessing or has accessed material prohibited above. The District's goal in creating the above standards and reporting requirement is not to create an environment of fear and apprehensiveness for users accessing the Internet and internal networks, but to affirmatively set forth content standards for users to be mindful of when accessing these resources on their own.

4. The District will fully cooperate with requests from law enforcement and regulatory agencies for logs, diaries, data, and archives on individuals' computing activities.

Blocking Sites

1. The District reserves the right to block sites that do not enhance classroom activities and/or career development.
2. Users are encouraged to contact the technology coordinator should any one inadvertently access a site that is inappropriate for the school setting.

Removing the Filter

1. Removing a site/activity from the blocked list will require a high level of justification. Anyone wishing that removal will submit a request in writing to the building administrator. A committee will review the site/activity in question. The committee shall be composed of the following:

    a. Building administrator
    b. Technology committee member
    c. Technology coordinator

2. The decision to remove the block on the site/activity will be based on the following criteria. Each of the criteria will be judged using contemporary community standards.

    a. Does the educational value of the site/activity significantly outweigh the inappropriate nature of the site/activity?
    b. Does the site/activity significantly enhance the curriculum?
    c. Can the material/information be obtained from other more appropriate sources?

3. Individuals will be notified of the approval or disapproval of the request in a timely manner. If the removal of the site/activity is granted, the committee will further indicate the length of time the block is to be removed.

All students and parents will sign an agreement/consent form annually. (Policy #743-Exhibit). The policy will be included annually in each building Faculty/Staff Handbook.

The Board authorizes the Administration to prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on instruction and student achievement.

CROSS REFERENCE:	Policy #743- Exhibit - Student Agreement/Consent Form – Acceptable Use of Networked Computers, Electronic Mail, and Internet Safety Policy Policy #744 - Creating and Placing Web Pages Policy#744-Exhibit—Consent Form Web/RVTV Permission to Display Classroom/Academic Activities Policy #726 Bullying / Cyber Bullying CIPA, N-CIPA, Protecting Children in the 21st Century Act FCC Rule 01-120 FCC Rule 11-125 River Valley School District Chromebook 1:1 Program: Procedures and Guidelines

APPROVED:	March 11, 1999
REVISED:	February 19, 2001
APPROVED:	March 8, 2001
REVISED:	April 29, 2004
APPROVED:	May 13, 2004
REVISED:	April 7, 2008
APPROVED:	May 12, 2008
REVISED:	September 11, 2008
APPROVED:	November 13, 2008
REVISED:	February 12, 2009
APPROVED:	February 26, 2009
REVISED:	August 12, 2010
APPROVED:	September 9, 2010
REVISED:	November 17, 2011
APPROVED:	December 20, 2011
REVISED:	December 12, 2013
APPROVED:	January 9, 2014
REVISED:	January 12, 2017
APPROVED:	February 9, 2017