522.7 RULE – NETWORK AND INTERNET ACCEPTABLE USE AND INTERNET SAFETY GUIDELINES FOR STAFF

The WRPS District Network (WRDN) and the Internet represent powerful educational resources, which allow users to find, use, and place information on the worldwide electronic network. Users will have the ability to connect many networks worldwide including: major universities, national libraries, other schools, and businesses. They will use these resources to communicate with others in those settings. The term WRDN will be used to refer to all wiring, equipment, software, computers, telephones, printers, copiers, connections, and services owned, leased, or contracted by the District to support educational and/or administrative functions.

WRPS has conduct standards for all users that detail appropriate school behavior, outline rights, and set expectations for users. Because the WRDN and the Internet are used to perform job duties, conduct standards apply. These conduct standards apply to an intent of vandalism of computer equipment, unauthorized access to information, computer piracy, hacking, electronic harassment, abusive and/or obscene language, and any tampering with hardware and software. It is the intention of the District that these guidelines provide awareness as well as education and guidelines for acceptable use and Internet safety. In addition, the policy identifies examples of acceptable and unacceptable use of district technology and the Internet. These guidelines will apply to all district employees and guests using the WRDN. Student acceptable use policy and guidelines will reference policy 365.1 NETWORK AND INTERNET ACCEPTABLE USE AND INTERNET SAFETY GUIDELINES FOR STUDENTS.

New District employees will be required to complete the WRDN Employee Acknowledgement and Waiver form. The signed statement acknowledges the receipt of the policy and the monitoring of the users network and Internet activity. Annually, each WRPS staff member will be notified and required to review the policy and verify that the review is completed to the Human Resources Department. This process will acknowledge the receipt of the policy and the monitoring of network and Internet activity.

Using Resources

The WRDN and the Internet represent a significant change in the way information is used and communicated. Technology changes rapidly and concerns with it and its implementation cannot be anticipated. The following guidelines attempt to deal with the known and emerging technology concerns in a manner consistent with current district practices and policies.

Using the WRDN

Do:

- Follow proper procedure for utilizing district resources (hardware, software, and services).
- Use district resources for educational purposes.
- Use complex passwords and change passwords regularly. WRPS is not liable due to compromised passwords.
- Lock your work station when not in proximity.
- Save your work often, WRPS will not be responsible for lost data.
- Logoff properly when finished.
- Properly power-down equipment when complete.

- Close programs that are not being used.
- Manage and organize network drives (delete files that are no longer needed).
- Use print resources responsibly (no classroom sets, use cut and paste).
- Use district owned devices to access internal WRDN resources.
- Use personal devices to connect to the WRPS Guest Network. This will be a filtered, Internet only connection.
    - WRPS Technology Support will not support personally owned computers or electronic devices.
    - Internal resources such as network file access and printing are not supported.
    - WRPS is not liable for any physical damage, loss, or theft of the device.
    - The District is not obligated to install data or electrical cabling.
    - Users of personally owned computers agree to maintain current antivirus software and agree to any WRPS security policies and settings that are required.
    - Any person who uses a personal device to access the WRPS Guest Network agrees to be responsible for and to reimburse WRPS for any intended damages.

Do not:

- Tie up the WRDN with non-school related activities.
- Play non-educational games on the WRDN or the Internet.
- Download files without permission.
- Download files for personal use.
- Access, distribute, or modify confidential or unauthorized information beyond job duties.
- Print or copy items for personal use.
- Share your network password or use another’s password.
- Install programs without permission from the Technology Support Department.
- Register for any on-line or real-time subscription/data services that do not relate to education.
- Purchase hardware or software without completing the Technology and Software Purchase Request Form.

The School District Network

The WRDN provides access for the purpose of fulfilling the district's mission of teaching, learning, and public service operations. The WRDN creates an environment to share information, access resources, and communicate. In addition, the WRDN serves as the district's connection to the Internet to support educational and administrative activities for district staff, students, and community members. Access to the WRDN and the Internet is a privilege and not a right. A WRDN account will be granted to all staff members to provide access to hardware, software, information technology systems, and the Internet. When staff is no longer employed by the district, accounts will be disabled for 30 days and then deleted.

The Internet and Internet Safety

The Internet is a global network made up of many smaller contributing networks, of which WRDN is a part. The Internet supports the open exchange of information among many different institutions all over the world. This system provides immediate access to information. Understanding the Internet and using it appropriately will allow users to develop 21st century skills to share resources, innovate, and communicate. Before using these research tools, it is important to understand the many issues related to Internet use. The moral and ethical issues relating to the use of worldwide information systems are controversial. The issues involve free speech, intellectual freedom, and access to information we deem appropriate according to our district and community standards. The intent of WRPS is to use connections on the Internet only for purposes consistent with our approved curriculum and/or administrative functions. However, making Internet access available to students and staff also brings with it the potential that some content may be controversial and of potential harm. Present technologies do not allow the District to filter out all of the materials that are unacceptable for users and intentionally accessing such materials in any form is strictly forbidden. If there is a question or concern regarding any of the information found on the Internet, staff should contact the Technology Support Department or a building administrator. The following Internet Safety guidelines along with the restricted Internet uses listed above serve as policy to be enforced by the district:

A: Inappropriate Data. Avoid obscene material, obscene performances, and sexual conduct that are harmful to minors. This includes content such as a picture, film, writing, or other recording that:

- the average person, applying contemporary community standards, would find the content offensive, distasteful, and/or objectionable
- under contemporary community standards, describes or shows sexual conduct in an offensive way; and
- lacks serious literary, artistic, political, educational or scientific value, if taken as a whole.

For a full definition of “obscene material,” “obscene performance,” and “sexual conduct,” reference Wisconsin Statute Section 944.21.

B: Privacy and Disclosing Information. The WRDN and the Internet are “public places.” Users must remember this space is shared with many other users and can be monitored. If a particular service is used on the network, chances are someone could find out about the connections made and what was looked at while in the system. When using the WRDN to communicate with others, keep the following in mind:

- you cannot see them;
- you cannot determine age or gender;
- information shared may be false;
- absolute privacy cannot be guaranteed in a network environment;
- think carefully about the content and the context of what is communicated;
- it is inappropriate to misrepresent your identity or purpose while using the WRDN.
- do not reveal Personal Identifiable Information (PII) to protect people’s personal safety. PII includes first name, last name, address, e-mail address (or other online contact information or a stream name that reveals an e-mail address), telephone number, Social Security number, a persistent identifier such as a customer number held in a cookie or a processor serial number, or any other information such that the combination permits physical or on-line contact. PII of students is not to be disclosed or used in any way on the Internet without the permission of a minor student’s parent/guardian or adult student. Students may not provide PII while on a district computer unless permission is given by a staff member. (e.g. Wisconsin Career Info System, online curricular projects such as Cyber Surfari.) Before granting permission, the staff member must review the site’s privacy policy for compliance with Children’s Online Privacy Protection Act (COPPA) and seek parental permission if necessary. Only sites that comply with the Children’s Online Privacy Protection Act (COPPA) will be considered for use within the district. Since COPPA only applies to children 12 and under, every effort should be made to use only sites that extend COPPA compliance to all students. No third-party service that discloses of PII is acceptable. If the company shares PII or reserves the right to share PII with third parties, the web site is not acceptable for use by WRPS students. In addition, sites that do not purge collected information should be avoided.

C: Criminal Behaviors. Using the WRDN and Internet access to gain and/or attempt to gain unauthorized access to other computer systems is prohibited. The activities include engaging in any illegal act as defined by the violation of local, state, federal statutes/laws. State Statute Section 943.70(2) states that “it is unlawful to copy, modify, destroy, access, or disclose restricted access codes regarding computer data or programs to unauthorized persons.

This also includes acts of someone who willfully, knowingly and without authorization modifies, destroys, accesses, takes possession of or copies data, computer programs, or supporting documentation, or modifies, destroys, uses, or takes equipment or supplies used or intended to be used in a computer, computer system or computer network". Users of WRDN are prohibited from disclosing their network access codes and allowing any other user to log in under their credentials. Any user committing acts of this kind may face disciplinary action by the school district including legal action. The user will be punished to the full extent of the law. Some examples of offenses are removing another user's accounts, changing other user's passwords, using an unauthorized account, damaging any files, altering the system, using the system to make money illegally (or for financial gain), arranging for a sale or purchase of illegal substances, engaging in criminal gang activity, "hacking" and other illegal activities.

D: Copyright and Plagiarism. Plagiarism is prohibited. Plagiarism is defined as "taking ideas or writings from another person and offering them as your own." In addition, a creator who leads readers to believe that what they are reading is the creator's original work when it is not is guilty of plagiarism. Credit must be given to the author through citations.

Copyright - "Fair Use" allows creators to use any legally found information on the Internet as long as the purpose was done in a scholarly intent. Considerations need to be given related to the amount of content, type of content, type of media, and the intended use. Fair use of digital content has not yet been clearly defined in statutes, therefore caution is recommended. Copyright law does not allow the re-publishing of text or graphics found on the Internet or file servers without written permission. Please follow the guidelines listed below as it relates to computer software copyright restrictions:

- All software programs used on the district network must be legally licensed;
- School resources/programs may not be used on home or personal computers without licensing consent;
- Personal software may not be loaded on school computers.

Further information regarding copyright may be obtained in the WRPS Copyright and Fair Use Handbook, A/V Director, or district Library Media Specialists.

E: Content Restriction Measures. The District uses technologies to filter Internet sites that are obscene and/or serve no educational purpose. Internet filtering tools are best effort tools to filter unsuitable sites. It is important to note that it is impossible to control access to all objectionable material. Every staff member must take responsibility for his or her use of the Internet and avoid sites and activities that are inappropriate or objectionable.

F: Cyber-bullying. WRDN should not be used for the purpose of harassment or cyber-bullying. Cyber-bullying is the use of any electronic communication device to convey a message in any form (text, image, audio or video) that defames, intimidates, harasses or is otherwise intended to harm, insult or humiliate in a deliberate, repeated or hostile and unwanted manner under a person's true or false identity. Any communication of this form which disrupts or prevents a safe and positive educational environment will be considered cyber bullying.

G: Internet Safety Instruction. The school district will provide instruction related to Internet safety. The curriculum will be taught within information technology courses, as well as integrated into regular classroom instruction. The content will cover digital citizenship topics related to Internet safety, copyright/plagiarism, and social networking.

Electronic Libraries and Online Resources

The Internet provides a vast digital library. Electronic databases and information search tools are an integral part of school library media centers and classroom. These tools are available as services on the WRDN. Users have the right to information, but the school has the right to restrict any information that does not support the approved curriculum and/or administrative functions. The following items need to be considered when using online resources:

Site Security - Web based companies must assure that they have taken steps to secure any data that has been given to them by WRPS users.

Compatibility - The site must provide acceptable technical performance, support, and compatibility with the local WRDN infrastructure.

Advertising - Current selection policies discourage advertising in curricular materials. Avoid web sites that feature advertising promoting activities that would be illegal or inappropriate for students (gambling, drinking, sexually explicit, etc.). When a teacher suspects that inappropriate advertising may appear on student screens (e.g. students are researching casino gambling), the teacher should pre-teach for appropriate student response. Whenever possible, encourage use of kid friendly search engines such as Yahoo Kids, Ask for Kids, Kids Click, Searchasaurus, etc. Seek sites that have been reviewed for student use and avoid sites that offer to sell products/services or are obtrusive. Library staff can assist with this process.

Contracts/partnerships - Contractual agreements with web based companies may only be entered into by an authorized administrator within budget constraints. Objectionable clauses must be open to negotiation. Ownership of any data created by WRPS users shall remain the property of the user or WRPS as appropriate. No changes can be made in the contract without the consent of WRPS authorized administrator. The District should not enter into exclusive contracts or restrict WRPS users from existing “fair use” provisions of the law.

Educators Using Social and Educational Networking Site

Social networks and educational networks are rapidly growing in popularity and use. As an educator, one must be diligent to uphold a professional image both offline and online. Do not be mistaken that being online shields a person’s personal life from being examined. An educator’s online identity can be very public and can cause serious consequences if behavior is careless. The concepts of social networking and the phenomenon of “friending” (creating a group of contacts that share interests, news, and personal views) have the potential of jeopardizing student and teacher dynamics. By “friending” students, teachers provide more information than one should share in an educational setting, including but not limited to providing students access to a teacher’s network of friends and acquaintances. It is important to maintain a professional relationship with students and avoid biased classroom relationships. The District does recognize the value of student/teacher interaction regarding the use of educational networking sites. Collaboration, resource sharing, and student/teacher dialog can be facilitated by the appropriate use of educational networking tools. In addition, it is important to separate professional social network profiles from personal social network profiles. In the education setting, a separate professional profile must be created and used for its professional purposes and manner. The following guidelines and best practices shall be followed to uphold professionalism.

- **Guidelines for the use of <u>personal</u> social networking sites by staff.**
  - Do not accept students as friends on personal social networking sites, i.e. Facebook/Myspace. Decline any student initiated friend requests.
  - Do not initiate friendships with students when using your personal profile.
  - Use caution when sharing information because people classified as "friends" have the ability to download and share your information with others.
  - Post only what you want the world to see. The content can be viewed by many audiences including: students, parents, administrators, and community members. Please be advised that the content will be available upon posting it and in the future even if the content is deleted.
  - Do not discuss or post comments regarding students, coworkers, or administrators.
  - Do not publically criticize school policies or personnel.
  - Visit your profile's security and privacy settings. At a minimum, educators should have all privacy settings set to "only friends." Typically, "friends of friends" or "networks and friends" open your content to a large group of unknown people. Your privacy and that of your family may be at risk.
- **Guidelines for the use of <u>professional</u> educational networking sites by staff.**
  - Create a separate professional profile that can be used strictly for classroom professional use only.
  - Professional use should be separate from personal use.
  - Do not say or do anything that you would not say or do as a teacher in the classroom. (Remember that all online communications are stored and monitored.)
  - Have a clear statement of purpose and outcomes for the use of the networking tool.
  - Establish a code of conduct for network participants.
  - Do not post images containing students without first verifying the parental photo release.
  - Pay close attention to the web site's security settings and allow only approved participants access to the site.
- **Guidelines for all networking sites by staff.**
  - Do not use commentary deemed to be defamatory, obscene, proprietary, or slanderous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.
  - Weigh whether a particular posting puts your effectiveness as a teacher at risk.
  - Due to security risks, be cautious when asked to install external applications that work with the social networking site. Only legitimate applications will be installed once a WRPS helpdesk ticket has been created.
  - If using a personal computer to access a social or educational networking site, be sure that your antivirus software is updated to prevent infections of spyware and adware.
  - Be careful not to fall for phishing scams that arrive via e-mail and/or on your social/educational network. Phishing scams are typically in the form of a link for you to click, leading to a fake login page.
  - If staff members learn of information on the social or educational networking site that falls under the mandatory reporting guidelines, they must report it as required by law.

<u>Web Page Guidelines</u>

The Technology Support Department shall be responsible for maintaining the official district web site and monitoring district web page activity. The purpose of the District's web site is to provide an instructional resource for students and district employees, a vehicle for communicating information about the Wisconsin Rapids Public Schools to the public, and having a general presence on the Internet.

Only web pages specifically maintained in accordance with board policy and established procedures shall be recognized as official representations of the District or individual schools. Information recognized as official representations of the District may only be placed on the official district web site or other approved sites.

Any web page that may be construed to be an official representation of the Wisconsin Rapids Public Schools or its programs must adhere to the following guidelines:

- The information and page layout has been reviewed and approved by the Director of Technology or designee.
- The information is an accurate and factual representation of official school and/or board policies, programs and positions. No personal, non-school related materials will be placed on the official District web site.
- The information does not contain confidential materials or other materials in violation of laws, regulations, or established board policies. Copyrighted material may not be used without permission. Posting content containing names, addresses, and pictures should be treated in a sensitive manner due to security and safety issues.
- The information is written clearly and meets proper standards of grammar, spelling and punctuation.
- The information and links are reviewed on a regular basis to ensure that they remain accurate and up-to-date.
- Only approved school related links will be placed on the official District web site.
- Web page designs must be consistent with district web page style sheets.
- Faculty web pages should have strong and pure educational purpose.
    - No obscene, degrading, or illegal content may be posted.
    - Content is not prescreened but must adhere to faculty webpage guidelines. Faculty web page guidelines can be accessed at the following URL: http://media.wrps.org/Training/faculty.html.
    - Student photo release must be signed and on record.
    - Student photos should not be published with student names. Should a staff member want to publish student photos with student names, a separate release form explaining the intent should be used.
- WRPS reserves the right to remove content.

Electronic Mail Guidelines

The Network Manager shall be responsible for maintaining the WRDN electronic mail system. Electronic mail (e-mail) is an electronic message sent or received by students or district employees for educational/communications purposes.

Due to the frequent use as a communication tool**,** WRPS will provide district employees with an e-mail account. Staff access to e-mail on WRDN will be through the district provided account and also commercial e-mail services for personal e-mail use.

All district assigned e-mail accounts are owned by the District and, therefore, are not private. Messages received by the e-mail system are retained. Contents of e-mail may be subject to Wisconsin Public Record Law (Wis. Stat 19.31-19.39). The Network Manager will establish mailbox size limits and all users should manage their mailbox by removing old messages in a timely fashion. The Network Manager will not routinely inspect the contents of e-mail sent by district employees. When staff is no longer employed by the District, accounts will be disabled for 30 days and then deleted.

Users of district e-mail accounts are expected to adhere to the following guidelines:

- All e-mail accounts will be protected by a manual log-in and individual password.
- WRDN e-mail should not be used to mass e-mail WRDN distribution lists unless pre-approval has been given by the Superintendent’s Office.
- Use of e-mail for financial gain is prohibited.
- Occasional personal use of e-mail is permitted, however it is strongly recommended that personal content not be mixed with official school business. It is also recommended that personal e-mail be sent and received via commercial e-mail services during time that does not interfere with the user’s professional responsibilities.
- Immediately delete inappropriate e-mail that you receive. Do not forward or reply to inappropriate e-mail messages.
- Do not use an account assigned to another user, forge e-mail messages, or post anonymous messages.
- Allowing another person to use your e-mail account is prohibited.

- Do not send messages that violate district policy, discloses personal information without authorization, or may be discriminatory, harassing, offensive, or contain material that defames an individual, company, or business.
- Log-off of your e-mail when finished.
- Student access to a listserv is by teacher permission only.
- Student access to chat rooms/videoconferencing is by teacher supervision only.
- Printing of e-mail messages is limited to educational or administrative functions.
- E-mail messages that may be viewed as a representation of the Wisconsin Rapids School District must be consistent with existing policy regarding district communication.

Questions or concerns on the proper use of the resources should be directed to the appropriate building administrator, the Network Manager, or the district Technology Director.

IP Telephone System

- Users of voicemail should keep their greeting messages current, check for incoming messages on a regular basis, and respond to them in a timely manner.
- Voicemail is volatile. If a voicemail is deleted, it will not be restored.
- Extensions are assigned to locations and are subject to change.
- Phones are only to be moved when necessary and the move process must be completed by the Technology Support Department.
- Currently, the phone system is configured to allow staff to dial long distance. Long distance should be used for educational purposes. Long distance usage will be monitored and modified as needed.
- User customizations of phone options are volatile.

Equity Concerns

Current selection policies discourage the use of biased materials. Avoid web sites that discriminate on the basis of age, gender, color, religion, national origin, ancestry, creed, pregnancy, marital or parental status, sexual orientation, or physical or mental, emotional, learning disability, or handicap. When such sites are accessed for an educational purpose (e.g. researching hate crimes), the teacher should pre-teach for appropriate student response.

Provisions must be made for those students who do not have Internet access at home and in some cases at school. Alternatives to Internet based activities need to be provided for students who don’t have access outside of school.

Accommodations need to be considered for special needs students.

Adoption: Approved by District Information and Technology Literacy Committee, Superintendent, School Board.

Distribution: On paper to staff and students. Policy and guidelines will also be available on the district web-site.

Revision: The District Information and Technology Literacy Committee will periodically review and maintain this policy and guidelines. Requests for policy changes should be forwarded to the District Technology Director.

APPROVED: March 11, 1996

REVISED: May 10, 1999
May 14, 2001
February 2004
` April 10, 2006
February 11, 2008
August 8, 2011