District Network Use Policy

This Internet Safety Policy ("Policy") has been put in place to: prevent unauthorized access and other unlawful activities by users on the network and online; prevent unauthorized disclosure of or access to personal and other sensitive information; and to comply with the Children's Internet Protection Act ("CIPA"). As used in this Policy, "user" includes anyone using the District's "network," which includes but is not limited to all wired and wireless computers, Internet access points, email, peripheral equipment, and any other forms of direct electronic communications or equipment provided by the District or when accessed by a District device. When connecting to the network on a personal device such as a laptop or cell phone, the user is subject to the rules and regulations set forth in this Policy. Only current students and District staff are authorized to use the network.

The District uses technology protection measures to block or filter, to the extent practicable, access of visual depictions that are *obscene, pornographic, and harmful to minors* over the network. The District reserves the right to monitor a user's network activities and to access, review, copy, store, or delete any electronic communication or files and disclose them to others as it deems necessary. A user should have no expectation of privacy regarding his/her use of District property, network and/or Internet access or files, including email.

1. **Access Policy**

   Access to the network is provided solely for educational purposes. All currently enrolled students will have access to the network and the Internet unless an exception/opt out form is filled out and signed by the parent/guardian. Once the form is signed by the parent/guardian and returned to the school, the student will be deactivated as a user and the student will have no access privileges to the network. By using the network, a user has agreed to adhere to the terms and conditions as listed in this Policy. This Policy is in the student handbook, and is a binding agreement. Access and use of the network is a privilege, not a right. A student may lose the privilege of using the District's network due to violation of this Policy, as determined by the District. If a user is uncertain about whether a particular use is acceptable or appropriate, he/she should consult a teacher, supervisor, or other appropriate District personnel.

   All District staff are expected to reasonably monitor and moderate student activities on the network and help ensure that the student follows District guidelines for Internet use. A student under the age of eighteen should only access District accounts outside of school if a parent/guardian supervises

his/her usage at all times.

2. **Unacceptable Uses of the Network or Internet**
The following are examples of inappropriate activity on the District network. The District reserves the right to take immediate action regarding activities that:
   a) create security and/or safety issues for the District, students, employees, schools, network or computer resources;
   b) expend District resources on content that the District, in its sole discretion, determines to lack legitimate educational content/purpose;
   c) reveal or have the potential of revealing on the Internet any personal information about him/herself or other persons. For example, a user should not reveal his/her name, home address, telephone number, or display photographs of him/herself, or others;
   d) reveal any user names or passwords to others;
   e) would allow a student to meet, in person, an individual he/she has only met on the Internet;
   f) violate any state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind; obscene depictions; harmful materials; materials that encourage others to violate the law; confidential information; or copyrighted materials;
   g) commit criminal activities that are punishable by law (e.g., unauthorized use or copying of information and downloading of music);
   h) sell or purchase illegal items or substances;
   i) post, send or store information online that could endanger others (e.g., bomb construction, drug manufacturing);
   j) obtain and/or use anonymous email sites; spamming; spreading viruses;
   k) cause harm to another person or damage to his/her property, such as:
      1) use profane, abusive, or impolite language; threaten, harass, or make damaging or false statements about another person; or access, transmit, or download offensive, harassing, sexist, racist or disparaging materials;
      2) delete, copy, modify or forge another person's user names, emails, files, or data; disguise one's identity, impersonate another user, or send an anonymous email;
      3) damage computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting the network or any computer system performance;
      4) use any District computer to conduct hacking, cracking, or vandalizing of programs or computers internal or external to the District, or attempt to access information protected by privacy laws; or
      5) access, transmit or download large files, including "chain letters" or

any type of "pyramid schemes."

6) engage in uses that jeopardize access or lead to unauthorized access into another person's accounts or other computer networks, such as:
   a. Use another person's account password(s) or identifier(s);
   b. Interfere with another user's ability to access his/her account(s); or
   c. Disclose another person's password to others or allow others to use another person's account(s).
7) attach unauthorized equipment to the District network;
8) download, install or use games, audio or video files, or any other applications without permission or approval by an Information System's staff member;
9) use the network or Internet for commercial purposes:
   a. personal financial gain;
   b. personal advertising, promotion, or financial gain; or
   c. conduct for-profit business activities and/or engage in non-government related fundraising or public relations activities such as solicitation for religious purposes or lobbying for personal political purposes.
10) the District determines as inappropriate.

3. **Special Considerations**

a) Anti-Cyber Bullying

Cyber bullying, which is sometimes referred to as online social cruelty or electronic bullying, is a new issue facing students. The District recognizes the important role that it has in keeping its students safe online both in the classroom and at home. Most instances of cyber bullying move from online to the classroom creating a negative learning environment. Many forms of cyber bullying fall under the auspices of this Policy; however, the District feels it is important to address this new issue directly. Acts of bullying which originate from outside the school (e.g., home) using the network or other means and which affect a student's studies at school are subject to investigation and, if necessary, discipline by the District.

b) Social Media

Use of any social media, (e.g., forums, chat rooms, instant messaging, Facebook, MySpace, Twitter, and other forms of direct electronic communication, etc.) is limited to educational use only. The District recognizes the importance of healthy communication and collaboration, and the use of social media should be used only in a responsible fashion, and in accordance with this Policy.

4. **Organizational Responsibility**

The District makes no guarantees, and none should be implied, about the

quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the District network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user.

The District also does not make any warranty for the accuracy or quality of the information obtained through user access or use of the network. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees. The student's parent/guardian is responsible for monitoring the minor's use of District resources from the home. It is suggested that parents/guardians use this document as a guideline of what is acceptable for their student at home as well. Additionally, the District does not warrant the effectiveness of the technology measures in filtering or blocking inappropriate content.

5. **Penalties for Improper Use or Violation of this Agreement**
The use of a District account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. All users of the District's electronic resources are required to comply with the District's policy and procedures. Violation of any of the conditions of use explained in this Network Use Policy could be cause for disciplinary action, including suspension or expulsion from school and suspension and revocation of network and computer access privileges. Disciplinary action will be taken against users found in violation of the rules of this document. All illegal activities will be reported to the police and full cooperation from the District will be given.

6. **Education**
It shall be the responsibility of all members of the District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the network and the Internet in accordance with this Policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The District or designated representatives will provide age appropriate training for users who use the District network. The training provided will be designed to promote the District's commitment to:
a) The standards and acceptable use of the network and the Internet services, as set forth in this Policy;
b) User safety with regard to:
(1) safety on the Internet;

(2) appropriate behavior while on online, on social networking websites, and in chat rooms; and
(3) cyberbullying awareness and response.

c) Compliance with the E-rate requirements of the Children's Internet Protection Act("CIPA").

Following receipt of this training, the user will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Note: See also Policy 4245: *District Network Use Policy for Personnel*

Legal Reference:

Children's Internet Protection Act and Neighborhood Children's Internet Protection Act: 20 U.S.C. §6777

Protecting Children in the 21st Century Act: 15 U.S.C. § 6551.

Administrative Regulation adopted: January 22, 1996
Administrative Regulation reviewed: August 21, 2000
Administrative Regulation revised/renumbered: May 21, 2012

RACINE UNIFIED SCHOOL DISTRICT
Network Use Agreement

STUDENT

I understand and will abide by the above Network Use Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.

User Signature: _____ Date: _____

PARENT/ GUARDIAN
(Must be signed if the student is less than 18 years of age)

As the parent or guardian of this student, I have read the Network Use Policy. I understand that this access is designed for educational purposes. Racine Unified School District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for Racine Unified School District to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Parent/ Guardian's Name (please print): _____

Signature: _____ Date: _____