District Network Use Policy

This District Network 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 primarily for educational purposes. All current District personnel will have access to the network and the Internet. By using the network, a user has agreed to adhere to the terms and conditions as listed in this Policy. While reasonable personal use will be permitted, users should use non-District networks (e.g., home internet, cell phone provider, etc.) for extensive or recurring activities that are not related to educational purposes. Access and use of the network is a privilege, not a right. A user 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 appropriate District personnel.

   All District staff are expected to follow District guidelines for District network use.

2. **Unacceptable Uses of the District Network**
   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 without administrator approval;
c) reveal any District user names or passwords to others;
d) 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;
e) commit criminal activities that are punishable by law (e.g., unauthorized use or copying of information and downloading of music);
f) purposefully or knowingly circumvent District web filters (e.g., using proxy sites);
g) sell or purchase illegal items or substances;
h) post, send or store information online that could endanger others (e.g., bomb construction, drug manufacturing);
i) obtain and/or use anonymous email sites; spamming; spreading viruses;)
j) cause harm to another person or damage to his/her property, such as:
    1) use profane or abusive 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) transmit "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-secured network;

8) use the District network 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.
9) 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 and staff. The District recognizes the important role that it has in keeping its students and staff 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 user or 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, Twitter, and other forms of direct electronic communication, etc.) is primarily limited to educational use. 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. **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, loss of employment, and suspension and revocation of network and computer access privileges. All illegal activities will be reported to the police and full cooperation from the District will be given.

5. 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 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 online, on social networking websites, and in chat rooms; and
    3) cyberbullying awareness and response.
c) appropriate use of copyrighted material;
d) Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Note: See also Policy 5162: *District Network Use Policy for Students*

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, 2002
Administrative Regulation edited: June 26, 2003
Administrative Regulation revised/renumbered: June 18, 2012

Racine Unified School District
Network Use Agreement

Employee

I acknowledge receipt of this policy.

Employee Signature: _____ Date: _____