

## Student Technology Responsible Use Policy

### Purpose

The River Ridge School District recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills. To that end, we provide the privilege of access to technologies for student and staff use. Access to technology is a privilege, not a right, and as such, students must seriously consider the responsibilities associated with signing this user agreement.

- Technology provided for educational purposes that Support the mission, vision, core beliefs and goals of River Ridge School District (RRSD)
- Enhance the development of 21<sup>st</sup> Century Skills included in Common Core Standards
- Encourage innovation, communication, creativity, collaboration and problem-solving skills by providing access to current and relevant information
- Prepare students for college or career

### Definition of Technology

- Internet, shared network resources and external file storage devices
- Desktop, mobile computers, tablets and handheld devices
- Videoconferencing, televisions, projection systems and telephones
- Online collaboration, message boards, and email
- Copiers, printers and peripheral equipment
- Additional technologies as developed

### CIPA

RRSD is in compliance with the Children's Internet Protection Act (CIPA) and has installed technology protection measures for all computers in the school corporation. A technology protection measure is in place that blocks or filters Internet access. This filter protects against access by adults and minors to visual depictions that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors. The content filter does monitor the online activities of minors and may be reviewed when deemed necessary.

The Responsible Use Policy (RUP) applies to:

- School-owned technology on the RRSD Internet/network, on non-school networks and offline
- Privately owned technology that is connected to the RRSD internet/network and on privately owned networks while on school property

### Responsible Use

Users must abide by all school rules as outlined in the Student Handbook and this Responsible Use Policy. This policy outlines the guidelines and behaviors that all users are expected to follow when using technology. It is the responsibility of both RRSD and parents to help prepare students to be members of a digital society or digital citizens. A digital citizenship is defined as the norms of behavior with regard to technology use.

A digital citizen is one who:

1. Understands human, cultural, and societal issues related to technology and practices legal and ethical behavior.
2. Advocates and practices safe, legal, and responsible use of information and technology.
3. Exhibits a positive attitude toward using technology that supports collaboration, learning, and productivity.
4. Demonstrates personal responsibility for lifelong learning.
5. Exhibits leadership for digital citizenship.

## **Prohibited Use**

Unacceptable uses of school electronic resources include, but are not limited to:

1. **Accessing or Communicating Inappropriate Materials**—Users may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.
2. **Illegal Activities**—Users may not use the school district’s computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. RRSD and its employees and agents assume no responsibility for illegal activities of students while using school computers or school-issued electronic resources.
3. **Violating Copyrights or Software Licenses**—Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.
4. **Plagiarism**—Users may not represent as their own work any materials obtained on the Internet (such as term papers, articles, music, etc). When using other sources, credit must be given to the copyright holder. Users should not take credit for things they didn’t create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.
5. **Cyberbullying** – Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, and cyberstalking are all examples of cyberbullying. Do not send emails or post comments with the intent of scaring, hurting, or intimidating others. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.
6. **Misuse of Passwords/Unauthorized Access** –Users may not share passwords; use any user account/password that is not assigned to them; or attempt to circumvent network security systems.
7. **Malicious Use/Vandalism**—Users may not engage in any malicious use, disruption or harm to the school district’s computers, electronic devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.
8. **Avoiding School Filters**—Users may not attempt to use any software, utilities or other means to access Internet sites or content blocked by the school filters.
9. **Unauthorized Access to Blogs/Social Networking Sites, Etc.** – Users may not access blogs, social networking sites, etc. prohibited by school administration or the RRSD Technology Department.

Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.

10. **Degrade System Resources** - Users shall not use the network in such a way that would degrade the performance system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects, as determined by the supervising instructor or school administrator.
11. **Unauthorized Equipment** - Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the district network without permission from the school administration or RRSD Technology Department.

### **Privacy**

All computers, telephone systems, voice mail systems, electronic mail, and electronic communication systems are the district's property. The district retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with district's computer, telephone, electronic mail, and voice mail. Students and staff should have no expectation that any information contained on such systems is confidential or private.

### **Safety/Security**

1. All users are given accounts upon entry into RRSD. Any user account given is intended for the sole use of that user only. Each user is responsible for the security of the system. Passwords should not be shared. If a user shared a password with another, that user will be held accountable.
2. Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as web sites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.
3. Staff may post student pictures on district/ school/classroom "public" websites as long as the student's name or other identifying information is not included. Students' grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.
4. Many devices have the capability to record audio and video. It is best practice and common courtesy to ask permission before recording an individual or groups. The use of cameras in any type of electronic device is strictly prohibited in locker rooms and restrooms.
5. RRSD staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).
6. Students may be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

### **Damage/Liability**

Users may be responsible for compensating the school district for any losses, costs or damages incurred for violations of Board policies/procedures and school rules, including the cost of investigating such violations. The school district assumes no responsibility for any unauthorized charges or costs

incurred by users while using school district computers, devices, or the school network.

### **Terms of Use**

RRSD reserves the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, including suspensions or expulsion from school, for violations of this policy. Additionally, all handbook regulations apply to the use of the RRSD network, Internet, and electronic resources. Students may also be subject to legal action and prosecution by law enforcement authorities.

### **Disclaimer**

RRSD, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, RRSD is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.
2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.
3. Unauthorized financial obligations resulting from the use of RRSD electronic resources.

**Adopted:** July 13, 2016, Revised December 14, 2016, Revised May 10, 2017

**Related Policy:** 363.2 Safe and Responsible Use of the Internet & Other Technology Resources

## ACCEPTANCE AND COMPLIANCE OF RESPONSIBLE USE POLICY 363.21

### Examples of Responsible Use

I will:

1. Use school technologies for school-related activities.
2. Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline. Be courteous and respectful.
3. Not post any information that I would not want students, parents, teachers, or future colleges or employers to see (once something is online, it is available to the world).
4. Treat school resources carefully, and alert staff if there is any problem with their operation.
5. Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
6. Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
7. Use school technologies at appropriate times and in approved places, for educational pursuits.
8. Cite sources when using online sites and resources for research.
9. Recognize that use of school technologies is a privilege and treat it as such.
10. Be cautious to protect the safety of others and myself.
11. Help to protect the security of school resources.

### Examples of Unacceptable Use

I will not:

1. Use school technologies in a way that could be personally or physically harmful.
2. Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Responsible Use Policy.
3. Create a personal mobile “hot-spot” or utilize a “proxy site” for the purpose of circumventing network safety measures and filtering tools.
4. Create, distribute or deploy multi-user servers or gaming software on or within the RRSD network.
5. Engage in cyberbullying, harassment, or disrespectful conduct toward others.
6. Try to find ways to circumvent the school’s safety measures and filtering tools; intent to circumvent safety measures and filtering tools is a violation of this Acceptable Use Policy.
7. Use school technologies to send spam or chain mail.
8. Plagiarize content I find online.
9. Post or otherwise disclose personally identifying information, about others or myself.
10. Agree to meet someone I meet online in real life.
11. Use language online that would be unacceptable in the classroom.
12. Use school technologies for illegal activities or to pursue information on such activities.
13. Attempt to hack or access sites, servers, or content that isn’t intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

By signing below, we agree to the expectations and procedures as detailed on the previous pages.

---

Student Signature

---

Date