**6000 Series: Instruction**

**Acceptable Technology Use Policy**

The Ridgefield Public Schools provides open and reliable digital infrastructure and resources for students and staff to be ethical and skilled learners and users of information, media, and technology. Therefore, Ridgefield Public School students and staff need digital resources to learn and apply skills in relevant and rigorous ways. Staff and students use technology anywhere and anytime, including through the use of district assigned devices that are educationally appropriate and aligned to student educational needs. The District's technology enables all students and staff to communicate, learn, share, collaborate and create, to think and solve problems, and to personalize their learning and teaching.

The Ridgefield Board of Education directs the Superintendent and his/her designees to create strong digital educational systems that support innovative teaching and learning, provide appropriate staff development opportunities, and develop procedures to support this policy.

Ridgefield Public Schools provides computers, computer systems, software and other digital resources as well as network access privileges for students and staff to carry out the mission of the District in an environment that ensures up-to-date information, management, and communication services. Responsible use of these resources, both in and out of school, is expected of all students and staff.

Students and staff use the property of Ridgefield Public Schools, including the computers, computer systems, software and other electronic resources for those activities directly related teaching, learning and/or management. The equipment, infrastructure, and software, other digital resources and the network are not to be used for personal gain or illicit/illegal activity by any user.

All users are hereby made aware that the Ridgefield Public Schools monitors and stores digital records of use of computers, computer systems, networks, and any other forms of digital resources unless specifically protected by the federal or state law. Therefore, Ridgefield Public Schools reserves the right to bypass any or all individual or group passwords to determine the activity on any or all district-owned computers, computer systems, software, online systems, and any other electronic resources.

Infringement upon, or disrespect of, the rights of other members or users or violation of the Acceptable Use Policy may result in the loss of network privileges and other disciplinary action including, but not limited to, suspension, expulsion, termination of employment and/or referral to appropriate law enforcement agencies.

Legal References: Connecticut General Statutes

1-19 (b)(11) Access to public records. Exempt records.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public
11-8b Transfer or disposal of public records. State Library Board to adopt regulations. (46b-56 (e) ) Access to Records of Minors.
53a-18-2b Harassment in the first degree: Class D felony. (As amended by PA 95-143)
Connecticut Public records Administration Schedule V - Disposition of Education Records (Revised 1983).

18 USC § 25 10-2522 electronic communication Privacy Act
20 U.S.C. Sections 6777, No Child Left Behind Act
20 U.S.C. 254 Children's Internet Protection Act of 2000
47 U.S.C. Children's online Protection Act of 1998
Federal Family Educational rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P. L. 93-568, codified at 20 U.S.C. 1232g.)
Dept. of Educ. 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs.
Implementing FERPA enacted as part of 438 General Educ. Provisions act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Public Law 94-553, the Copyright Act of 1976, 17 U.S.C. 101 et. Seq.

**Policy adopted: April 11, 2016**

**6000 Series: Instruction**

**Acceptable Technology Use Regulation**

**Acceptable Technology Use Community Agreement**

These procedures are written to support the Acceptable Technology Use Policy of the Ridgefield Public Schools and to promote positive and effective digital citizenship among students and staff.

The district retains control, custody and supervision of all computers, digital resources, and data owned, subscribed to, or leased by the district. The Board of Education reserves the right to monitor all technology resource activity by employees, students, and other system users. Employees and students have no expectation of privacy in their use of school computers, including e-mail messages and stored files.

Employees and students are expected to use appropriate judgment and caution in communication concerning students and staff to ensure that personally identifiable information remains confidential.

**Terminology**

Technology Resources/Devices - Ridgefield Public School computers, tablets, e-mail, mobile devices, cell phones, networks, digital subscriptions, information/data systems, the Internet, peripherals, portal and any other technology-based tools.

Users – Anyone, including but not limited to staff, student, Board of Education, visitor/guest, consultant, or external vendor, that access the RPS technology resources.

**Safety**

To the greatest extent possible, users of technology resources will be protected from harassment and unwanted contacts. Any user who receives threatening or unwelcome communications should bring them to the attention of a teacher or administrator. Users must be aware that there are many services available on the Internet that could potentially be offensive to certain groups of users. The District cannot eliminate access to all such services, nor can they identify all of them. Individual users must take responsibility for their own actions when navigating the technology resources.

**Security, Filtering and Monitoring**

Security on the technology resources is a high priority. If users of the technology resources of the Ridgefield Public Schools identify a security problem, the user must notify a teacher or administrator at once without discussing it or showing it to another user.

Users must not use another individual's account. Any user identified as a security risk will be denied access to the technology resources of the Ridgefield Public Schools.

Filtering should be viewed as one of a number of techniques used to manage users' access to the Internet and encourage acceptable use. Internet filtering should not be viewed as a foolproof approach to preventing access

to inappropriate material. Occasionally, students and/or staff may access websites that are objectionable. These should be reported to the superintendent/designee for consideration to be blocked by the filtering system.

In accordance with the Children's Internet Protection Act, filters will be maintained to block websites deemed to be obscene, pornographic, and/or harmful to minors.

**No Expectation of Privacy**

The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information or any other data communicated, created, or accessed using district digital resources. No user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to state and federal public records disclosure laws.

**User Levels**

In an environment where learning can take place anytime and anywhere, the Ridgefield Public Schools is committed to providing age-appropriate teaching and learning opportunities for students to use technology tools. To facilitate that five user levels are defined for the purposes of organizing supervision for group instruction and personal use of these information resources. All employees must receive training on acceptable use of RPS technology resources annually at the start of the school year or at the time of hire.

Digital Citizenship is a curriculum framework to teach students to be responsible, legal, ethical, and safe in their use of digital resources. The district provides ongoing Digital Citizenship lessons to students.

| | Level 1 (PreK-2) | Level 2 (3-5) | Level 3 (6-8) | Level 4 (9-12) | Level 5 Adults |
|---|---|---|---|---|---|
| Use direct links off school/district website under adult supervision | X | X | | | |
| Use district technology resources under adult supervision | X | X | | | |
| Use links off teacher's online classroom management system (Google Classroom) under adult supervision | | X | | | |
| Use guided internet searches using approved search engine under adult supervision | | X | | | |
| Use assigned district personal learning device throughout school | | | X | | |
| Use website links, teacher provided links, and internet search engines independently | | | X | X | X |
| Teacher reviews Acceptable Use Policy start of year with students prior to use of technology | X | X | X | | |
| Student signs Acceptable Use Policy annually | | | X | X | |
| User signs Acceptable Use Policy annually | | | | | X |

The Superintendent will establish guidelines and standards for teacher posting of assignments and class information (hours, frequency, etc.).

The Superintendent will establish the protocol for annual acceptance of the Acceptable Use Policy by parents, students, staff, visitors, guests, and all other users. Annual acceptance by parents may be done through implied consent (receipt of policy with opt out of acceptance) or required signature.

**District Provided Personal Learning Devices**

Students in grades 6-8 will receive a Personal Learning Device each fall. Parents and students must sign and agree to the student device sign out sheet and guidelines provided by their respective schools. Devices will be collected prior to summer break and issued at the start of the school year. Parents are financially responsible for damages, loss, or theft of the device. Students who withdraw, are expelled, or terminate enrollment for any other reason must return their devices along with accessories on the date of departure.

**Personal Learning Device Temporary Sign-out**

Ridgefield Public Schools students who have the option of borrowing technology equipment are responsible for its use and condition. Devices are only borrowed during the school day and must be returned the same day.

**Personal Technology**

Some users are permitted to use personal devices while connected to the RPS wireless network. At the elementary schools, student use of personal devices is approved by the teacher based on educational goals. Use of personal devices is governed by the BYOT policy 6141.328.

Connecting personal devices to district computers (scanners, printers, mobile phones/tablets, etc.) is not permitted unless provided authorization in advance by the Director of Technology or designee. Connecting external drives (USB flash drive or equivalent) is permitted. Connecting to personal cloud resources to access data for educational uses is permitted.

Users are strictly prohibited from installing personal software onto any RPS device or RPS software on personal devices at any time without the prior authorization of the Director of Technology or designee. The use of district resources that do not get installed on a local device is permitted on personal devices.

Due to the confidentiality of student data, assessment data, employee data, and confidential organizational data, the downloading and storing of confidential data on personal devices is not permitted.

**Confidentiality and Data Guidelines**

The Ridgefield Public Schools abides by all state and federal laws with regard to student, staff, and organizational data. Guidelines, protocols, and service contracts are continually monitored and updated to ensure all data systems, cloud-based resources, locally installed applications, databases, and vendors protect and secure the confidentiality and privacy of student, employee and organizational data (Ridgefield Public Schools Data). This set of data includes, but is not limited to, student records, assessment data, family demographic data, employee data, and email.

Confidentiality and overall use of these online resources is protected by law, including the Family Education Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Ridgefield Public Schools Acceptable Use Policy.

- Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records and gives parents the right to review student records. Under FERPA, the school district or institution or

person acting on the behalf of the school district may maintain educational records, which includes records, files, documents, and other materials that contain information directly related to a student. School officials may only provide student records to third parties with the permission from the parent or eligible student. Directory information may be released if parents do not object to any disclosures.

- Children's Online Privacy Protection Act (COPPA) applies to commercial companies and limits their ability to collect personal information from children under 13. No personal student information is collected for commercial purposes. The district will annually inform parents and collect permission that allows the school to act as an agent for parents in the collection of information within the school context. Permission is granted by the acceptance of the annual Acceptable Use Policy. The school's use of student information is solely for education purposes. Student information that is "collected" is described as (projects, documents, email, files, username and password).

**District Guidelines and Expectations**

The Ridgefield Public Schools expects all employees and external service providers, acting on behalf of the Ridgefield Public Schools, to take all measures to protect student, employee, and organizational data. As such, the following guidelines and procedures are to be adhered to by employees, vendors, and service providers.

- All student, employee, and organization data (Ridgefield Public Schools data) is the property of the Ridgefield Public Schools.
- All computers, tablets, smartphones, cloud-based resources, or servers that store and/or have access to Ridgefield Public Schools data must be password-protected at all times when not actively in use by the user.
- All cloud-based resources, software, mobile device apps and 3rd parties with access to data must be approved for use by the Director of Technology or assigned designee. Approval for installation or use of these resources is dependent on educational appropriateness, compatibility with resources, availability of support, organizational needs, and adherence to the Confidentiality and Data Guidelines. The procedures for approval of resources and 3rd parties will be reviewed and communicated annually to staff and publicly posted on the district website.
- Ridgefield Public Schools data may be accessed via cloud-based resources and apps while on mobile devices or personal (non-RPS) devices, however such data may not be downloaded for storage on personal (non-RPS) technology.
- Access to and/or storage of Ridgefield Public Schools data must be purged and permanently deleted at the termination of employment, service contract/subscription, or consulting.
- Access to Ridgefield Public Schools data will only be provided after acceptance and signature of the Acceptable Use Policy, which contains the Confidentiality and Privacy of Data guidelines.
- Ridgefield Public Schools data is not to be shared with a third party, including parents or community residents, unless permitted by FERPA, COPPA, CIPA PPRA, or FOI and within the parameters of the type of data that may be released.
- Email containing personally identifiable student information may constitute an educational record and thus be subject to disclosure under FERPA and may, under certain circumstances, be subject to FOI. Staff must comply with FERPA in all email communication with anyone other than the parent(s) of the student or the eligible student

**District Publishing Guidelines**

Any distribution of educational records, including digital records, must comply with FERPA, district policies, and professional standards. District, school, and individual use of digital resources to distribute intellectual property, images, videos and information shall be related to school curriculum and instruction, school-authorized activities, and other information relating to school and district goals and ensure the safety and security of all students and staff.

- All distributed content shall follow the standards for ethical behavior in regard to information and communication technologies by showing respect for the principles of intellectual freedom, intellectual property rights, and the responsible use of the information and communication technologies.
- All distributed audio and video recordings of classroom activities shall follow ethical standards by posting content that has been recorded with the intent to be shared online and with permission by those being recorded.
- All content shall be age-appropriate to safeguard students by shielding the identification of students' identification and locations. Content may include names of individuals; however identifying information, such as names of family members, e-mail addresses, addresses and phone numbers will remain private.
- Content shall not contain objectionable material or point to objectionable material. The determination of what constitutes objectionable material shall be made on a case-by-case basis, as determined by the Director of Technology and a Building Administrator. The distribution of content shall follow district policy, copyright law, and fair use Guidelines.

**Copyright**

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 generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the air Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

**Responsibilities**

Users need to become familiar with their responsibilities while using the Ridgefield Public Schools technology resources.

**Users agree to always adhere to the following standards and expectations for conduct.**

1. **Behave ethically, safely, legally, and responsibly when using technology resources**
    a. Refrain from utilizing proxy gateways, or similar technologies, to bypass technology monitoring and filtering.
    b. Handle technology devices with care. Refrain from deleting, destroying, modifying, abusing, moving resources without permission, and/or accessing unauthorized technology resources.
    c. Do not breach or disable network security mechanisms, or compromise network stability or security in any way. or download/ modify computer software in violation of the district's license agreement(s) without authorization from the Technology Department.

d. Acceptable use of technology defined within the Acceptable Use Policy covers use of all Ridgefield Public Schools technology resources assigned to and used within schools and off-site.

2. **Use technology resources to transmit communications or access information only for legitimate educationally relevant purposes and to access educationally appropriate content**.
    a. Refrain from sending any form of communication that breaches the district's confidentiality and data privacy requirements, or the confidentiality of students.
    b. Refrain from sending any form of communication that harasses, threatens or is discriminatory.
    c. Refrain from accessing any material that is obscene, harmful to minors or prohibited by law.
    d. Refrain from using social network tools for personal use. Professional use and a student academic use is defined in RPS policies 4118.51 (4218.51) and 6141.322.
    e. Use communication and collaboration tools (email, voicemail, blogs, etc.) respectfully and professionally.

3. **Respect the privacy of others and treat information created by others as the private property of the creator.**
    a. Maintain confidentiality of your username and password by not sharing it with others and not using another person's username and password.
    b. Maintain the integrity of files and data by not trespassing, modifying, copying or deleting files of other users without their consent.
    c. Protect the confidentiality and safety of others when sharing work and images.
    d. Protect the privacy and confidentiality of students, staff and Ridgefield Public Schools by adhering to the Confidentiality and Data Guidelines.
    e. Share, post and publish only within the context of the District Publishing Guidelines.
    f. Respect copyright and fair use laws; these policies and procedures apply in digital contexts, as well. Plagiarism is prohibited.

4. **All technology assigned to staff, students, or visitors are property of Ridgefield Public Schools and are to be kept secure and in working condition.**
    a. Any device provided to staff or students by the Ridgefield Public Schools is the property of Ridgefield Public Schools and therefore must be returned to appropriate administrators, teachers, or Technology Department staff upon request.
    b. Upon departure from the Ridgefield Public Schools assigned devices are to be returned promptly to the Technology Department.
    c. Damaged and non-functioning devices are to be returned immediately to the Technology Department for repair.
    d. Staff and students are financially responsible for theft and damage caused by neglect or improper use.

**Consequences**

The Ridgefield Public Schools will not be responsible for unauthorized financial obligations resulting from the use of, or access to, Ridgefield Public School's computer network or the Internet. Ridgefield Public Schools

assumes no responsibility for any unauthorized charges made by employees including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

Users of the technology resources of the Ridgefield Public Schools shall be responsible for damages to the equipment, system and software resulting from deliberate or willful acts.

Illegal use of the technology resources of the Ridgefield Public Schools, intentional deletion or damage of files or data belonging to others, and copyright/fair use violations or theft of services will be reported to the appropriate legal authorities for possible prosecution and other consequences.

The employee or student shall be responsible for any losses, costs or damages incurred by the district related to violations of district policy or these regulations for which they are responsible.

Violation of the Acceptable Technology Use Policy and Regulation or in these procedures could be cause for disciplinary action, including suspension or revocation of network and computer access privileges of employees and students as well as other permissible disciplinary actions, up to and including expulsion or termination, as defined in other student and staff policies and administered by district administration.

**Regulation approved: April 12, 2016**