Responsible Use of Technology Policy

Purpose and Expectations

The Chariho Regional School District (“District”) uses technology as one tool to support our mission of ensuring that all students meet high academic standards and are prepared for lifelong learning and productive global citizenship. The District supports the notion that students and educators should have ready access to the vast instructional potential of technological tools.

The District's Responsible Use of Technology Policy (RUTP) provides guidance to students ("users") and their parents/guardians, and District employees (“providers”) in the responsible use of technology for educational purposes, research and communication. This policy provides guidelines but does not attempt to state all permitted or prohibited activities. The District has the right to prohibit any District technology use by providers and users not stated in this policy.

Every user needs technology skills and knowledge to succeed as an effective and productive citizen. Every provider needs access to technological tools to provide users with the best possible opportunity for success. The 21st-century learning environment includes all types of resources including computing devices, Internet sites and software. Users and providers have access to personal technology including, but not limited to, computers and cell phones and District technology which includes local network resources, Internet service, and a variety of digital devices including, but not limited to, laptops, tablets, desktop computers, smart boards and software. All use of District technology is intended to support the effective implementation of the District's curriculum, standards and business requirements.

Only educational software and digital tools approved by the District may be used for instructional purposes.

Internet Safety, CIPA and Personal Use

The District complies with the Children’s Internet Protection Act (“CIPA”). The District uses technology protection measures to block or filter, to the extent practicable, access to content or transmission of visual depictions, communications or otherwise, that are obscene, pornographic, and/or harmful to minors over the network. Providers, even when they allow access for educational reasons to sites normally blocked or filtered, also provide reasonable monitoring of users’ Internet use. It is the responsibility of all to monitor their own access and use sound judgment in matters related to potentially obscene, pornographic, and/or harmful materials. The District’s content filter will be frequently updated and be active when any District device is used outside of school and when any personal device accesses the Internet via the District’s network.

This policy applies regardless of whether such use occurs on or off school property and it applies to all District technological resources including, but not limited to, computer networks and connections; the resources, tools, and learning environments made available by or on the network; and all devices that connect to those networks. When issued a mobile computing device by the District, users and providers may use it at school or at home. The District permits personal use so long as it occurs on personal time and complies with this policy and CIPA. Personal use should not interfere with District activities and other established policies and procedures. Users and providers are responsible for their actions and activities involving District technology, networks, and Internet services and for keeping their files, passwords, and accounts secure. Users and providers accessing the Internet via District technology assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by the policy or accompanying guidelines. Damage, malfunction, theft, or similar event to an issued and assigned device must be reported within twenty-four (24) hours of the event.

Unauthorized Software and Hardware Modifications

Providers and users shall not install software or hardware on the District-issued devices that can monitor or record the Internet activity, access the files or electronic communications, or capture any data transmissions from other District or non-District-issued equipment. Additionally, hardware installation, repairs, and hardware configuration of the District-issued devices will be performed by the District IT staff or by authorized users or providers under the direct supervision and responsibility of District IT staff. All District technology, which includes software, is subject to District IT oversight and control.

Social Media

Personal or private use of social media may have unintended consequences. Social media is defined as Internet-based applications including, but not limited to, Facebook, Twitter, Instagram, Pinterest, Tik Tok, Snapchat, chat rooms, instant messaging, blogs, wiki's, etc., that turn communication into interactive online dialogue.

With regard to providers, postings to social media should be done in a manner sensitive to the providers' professional responsibilities and should maintain an appropriate professional relationship with users. The District authorizes providers to access social media from the District's network provided such access has an educational purpose.

With regard to users, social media may not be used in a way that undermines the District's mission or causes a substantial disruption to the school environment. Providers and Users are also bound by other District policies, such as the Personnel Management System Policy and the Standards for Student Behavior Policy.

Personal access and use of social media from the District's network and Internet service by users and providers is prohibited during instructional time, unless specifically intended for educational purposes.

All use of technology resources, including accessing social media with District property or during school-sanctioned events, shall be in accordance with all provisions of this policy.

No Expectation of Privacy with District Technology, Networks, or Internet Services

The District retains control, custody and supervision of all technology, networks and Internet services owned or financed by the District. The District reserves the right to monitor all usage including Internet usage of the District-issued equipment. Users and providers shall have no expectation of privacy with regard to the use of District technology and District property including network, Internet access or files and email. No expectation of privacy extends to all files stored on the District-issued device including email and Internet usage of the device.

The District reserves the right to monitor users' and providers' online activities accessed through District technology, including networks or Internet services. The District can access, review, copy, store or delete any electronic communication or files and disclose them to parents, guardians, teachers, administrators or law enforcement authorities as the District deems necessary or mandated by law.

The District will not remotely activate the camera or microphone for monitoring purposes. Activating the camera on a device may only be done by the student using the device. The District may, however, require a student to activate their camera when engaged in distance learning as it aligns with best practices for pedagogical purposes.

Other Guidelines for Users

A. Technology Use is at the Discretion of the District

Use of District technology, networks and Internet services can be restricted or prohibited. Users must also follow this policy when using allowable personal digital devices including, but not limited to, laptop computers, tablets and cell phones while on District property, at school-activities and/or riding District-provided transportation.

B. Responsible Use

1. Users are expected to use District technology primarily for educational purposes.
2. Users are expected to comply with this policy when using the technology outlined in this policy.
3. Users are responsible for their actions and activities involving District technology, networks and Internet services and for keeping their files, passwords and accounts secure.
4. Users shall not use personal devices during instructional time without permission.
5. Users should promptly inform their teacher or school administrator if they are aware of any technology issue that is contrary to this policy.
6. Users are expected to comply with any District requests to limit the use of the District technology.
7. Except when permitted by the provider, the expectation is that responses by users in assessments reflect the knowledge and ability of the user without the support from other people, aids or documents except as permitted by the teacher.

C. Prohibited Uses

While technology can be a valuable resource in an academic setting, it has the potential for misuse. Prohibited use will result in disciplinary action as defined by the appropriate Standards for Student Behavior Policy and other applicable policies and may also include loss of use of District technology.

1. Inappropriate Material: Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal.
2. Illegal Activities: Using District technology, networks and/or Internet services for any illegal activity or activity that violates other District policies, procedures and/or school rules.
3. Violation of Copyrights: Copying or downloading copyrighted materials without the owner's permission or any other activity that violates other District policies regarding copyrighted material.
4. Non-School-Related Uses: Using District technology, networks or Internet services for private financial gain, commercial, political, religious, advertising or solicitation purposes is prohibited.
5. Misuse of Passwords/Unauthorized Access: Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts or providers' accounts.
6. Malicious Use/Vandalism: Any malicious use, disruption or harm to District technology, including, but not limited to, modifying or uninstalling device configurations, hacking activities and creation/uploading of computer viruses. Vandalism includes damaging computer equipment, files, data or the network in any way.

7. Unauthorized Access of Electronic Communication Tools: Accessing resources such as email, chat, social networking sites, texting and telephone services without specific authorization from instructional staff.

D. Personalization of Issued and Assigned Devices

1. Users are allowed to personalize devices within the parameters of this policy. Personalization must not impede the instructional and educational use of the device and may not be any form of non-digital customization including, but not limited to, stickers, decals or artwork.
2. Users are not allowed to make configuration changes that may interfere with maintenance, software installation, or software upgrades.
3. Personalization must conform to all other applicable policies of the District. No use of media prohibited by other policies is allowed.
4. The District assumes no liability or responsibility for personal electronic property saved to a device. This includes, but is not limited to, personal software, files, games, eBooks, and other media.
5. The District assumes no liability or responsibility for unauthorized charges made by users that may include, but are not limited to, credit card charges, long-distance telephone charges, and electronic payment services.
6. In the event that the device's internal memory is insufficient for the download or use of required educational content, the provider and/or users will be required to remove personal files.

E. Communication of Policy

This policy shall be provided to all users and parents/guardians on an annual basis. All users shall be provided with instruction regarding this policy.

Other Guidelines for Providers

A. Primary Intent

District technology is made available to providers to allow for the enhancement, enrichment, and expansion of educational opportunities for users. Its primary use is for educational purposes.

B. Responsible Use

1. Providers are expected to use District technology primarily for educational purposes.
2. Providers are expected to comply with this policy and when using the technology outlined in this policy.
3. Providers are responsible for their actions and activities involving District technology which includes networks and Internet services, and for keeping their files, passwords and accounts secure.
4. Providers should promptly inform District IT staff or school administration if they are aware of any technology use or issue that is contrary to this policy.
5. Providers are expected to comply with any District requests to limit the use of District technology.
6. Providers should understand that they are held to a higher standard than the general public and are expected to set the example with regard to policy adherence, standards of conduct, and ethics. Reference should be made to other District policies, including the Personnel Management System Policy.

C. Prohibited Uses

1. Inappropriate Material: Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal.
2. Illegal Activities: Using District technology, networks and/or Internet services for illegal activity or activity that violates other District policies, procedures, and/or school rules.
3. Violation of Copyrights: Copying or downloading copyrighted materials without the owner's permission or any other activity that violates other District policies regarding copyrighted material. Under no circumstance may software purchased by the District be copied or distributed.
4. Non-School-Related Uses: Using District technology, including networks or Internet services for private financial gain, commercial, political, religious, advertising or solicitation purposes is prohibited.
5. Misuse of Passwords/Unauthorized Access: Sharing passwords, using other providers' passwords without permission and/or accessing other providers' or users' accounts.

D. Personalization of Issued and Assigned Devices

1. Providers are allowed to personalize devices within the parameters of this policy. Personalization must not impede the instructional and educational use of the device.
2. Providers are not allowed to make configuration changes that may interfere with maintenance, software installation, or software upgrades.
3. Personalization must conform to all other applicable policies of the District. No use of media prohibited by other policies is allowed.
4. The District assumes no liability or responsibility for personal electronic property saved to a device. This includes, but is not limited to, personal software, files, games, eBooks, and other media.
5. The District assumes no liability or responsibility for unauthorized charges made by providers that may include, but are not limited to, credit card charges, long-distance telephone charges, and electronic payment services.
6. In the event that the device's internal memory is insufficient for the download or use of required educational content, the provider will be required to remove personal files.

E. Communication of Policy

All providers shall be given instruction regarding this policy.

Revised 7-17-12-effective 8-29-12; Revised 7-16-13-effective 9-1-13; Revised and effective 12-16-14; Revised 5-12-15-effective 7-1-15; Revised and Effective 2-9-21; Revised and Effective 6-22-21