Reynoldsburg City Schools

Computer and Technology Acceptable Use Policy

Staff, Volunteers and Students

AUP Sections

The Reynoldsburg City School District ("The District") offers a variety of technology tools and networked computer access to all currently enrolled students and staff ("user(s)"). Many personally owned devices are being used to support and enhance the educational process. These resources and devices, whether District owned or personally owned, are used to provide students and staff support for the teaching and learning process. With this access comes the responsibility to insure proper usage of these resources. The District views technology as an integral part of the educational process to help increase productivity, achievement, organization, and learning opportunities. In order to maintain adequate resources, each user must be mindful about maintaining the hardware and software associated with The District. Use of District owned technology or network resources implies acceptance of this policy. Due to rapid change in technology, a user's access and/or this policy are subject to change at any time. Each user will be held responsible for compliance with the following guidelines:

1. **Acceptable Use:**
   Technology must be used to support education and research and be consistent with the objectives of The District. The computer network also supports the administrative and professional functions of the staff as well as efficiencies associated with electronic communication.

   • Transmission of any material in violation of any federal or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening, harassing, or obscene material, or material protected by trade secret.
   • Use for commercial activities by for-profit institutions is prohibited. Use for any kind of product or service advertisement, or political lobbying is also prohibited.
   • Installation of software not owned or authorized by The District is prohibited on District computers.
   • Staff and students are assigned a District e-mail account. The primary purpose of this account is to conduct school business. It is expected that all communication via The District owned email system is professional and school related. Electronic mail that is sent, received or stored on District equipment, may constitute a public record subject to disclosure under Ohio's Public Records Law, and may be subject to the Board's records retention policy. Assume no right to privacy.
   • Staff and students are assigned a Google for Education account. The primary purpose of this account is to conduct school business. It is expected that all communication and video footage transmitted via Google for Education services/apps such as Google Hangouts Meet, Google Hangouts, Google Docs, and Google Classroom be professional and school related, regardless of where or when the account is used. The use of school appropriate language is a requirement.
   • Users will be responsible for any unauthorized monetary charges incurred for purchases made with District technology or through the District's network.
   • Games are not considered an educational use of technology. Games may not be played when using technology tools within The District with the following exceptions:
      - Games that are created as part of an educational curriculum.
      - Games that directly support current curricular objectives.

2. Privileges:

Use of The District's network, devices, and accounts is a privilege, not a right, and inappropriate use may result in prohibition from further use, as well as disciplinary action up to and including termination/expulsion. District staff members have a responsibility to report and investigate observed inappropriate use. During the course of investigating inappropriate use, staff may access, view, and/or document histories, logs, files, computer screens, and electronic or wireless communications; privacy should not be assumed when using The District's network or devices.

Building principals and Central Office administrators may disable access, and or repossess a District owned device at any time. District staff may request the Information Technology Department ('IT Department") to deny, revoke, or suspend specific user rights and/or accounts.

3. Information and Internet Access:

In compliance with the Federal Child Internet Protection Act (CIPA) The District filters the Internet for inappropriate content. All devices accessing the Internet through The District's network receive filtered Internet content. District owned devices, even if used offsite, will only access the Internet through a District controlled content filter. CIPA requires "a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors."

Although Internet filters are very effective, there is no such thing as 100% perfect Internet filter technology. It may be possible for an inappropriate website to pass through the filter. Students should close any webpage deemed or which may reasonably be considered inappropriate, and tell a staff member what happened. Staff should report the Internet address (URL) of the inappropriate site to the IT Department by e-mail or submitting a Help Desk ticket.

The Internet is powerful educational tool. Individuals are responsible for Internet usage in accordance with all sections of this Acceptable Use Policy (AUP). Willful intent to bypass or compromise The District Internet filter is considered inappropriate use. Random searching for information which could result in the display of content that is obscene or harmful to minors, is inappropriate use. Bringing content into the District that would otherwise be filtered is also considered inappropriate. In addition, specific Internet sites may be added to or removed from the "Block List".

A critical part of using the Internet as a resource is for the user to learn how to determine the validity of information posted. Downloading information from the Internet should be done with caution. Just because it is posted, does not mean it is legal to download. Downloading media protected by copyright without paying for it legitimately is illegal. Students and staff need to familiarize themselves with copyright and fair use laws and guidelines (see section 8 of this AUP). Copyright violation is illegal, and in accordance with this policy is strictly prohibited.

4. Procedures and Caveats:

Files may be deleted in accordance with the District's records retention schedule, to make room for current project work. If you have older files you want to keep, you need to make a copy to external media or to a cloud storage location. If you need to keep a number of large files for an extended period of time on school equipment, please let a member of the IT Department know so that arrangements can be made (provided sufficient storage space is available).

Some large file types may be deleted in accordance with the District's records retention schedule if no educational value is apparent. It is the user's responsibility to keep folders free of files for which there exists no further use.

These may include, but are not limited to:

- **Movies (example files: .avi, .mov, .mpeg)**
- **Songs (example files: .wav, .mp3, .mid)**
- **Pictures (example files: .gif, .jpg, .jpeg, .bmp, etc.)**
- **Archives (example files: .zip, .ISO, .tar, .dmg, .rar, etc.)**

Viruses and Malware:

Malware is a term used to describe any software program whose intentions are to destroy or disrupt a system. The District has put in place security measures to protect District systems from the various forms of malware. Those measures include, but are not limited to: virus protection, behavior monitoring, network threat inspection, spam filtering, bolstered security settings, rapid deployment of security updates, and a firewall to protect The District's network from external threats. It is in The District's best interest to ensure that **personally owned** devices have sufficient virus protection, are free of malware, and have the latest security patches installed prior to granting these devices a network connection.

The District recommends that all staff, students and parents consider implementing three basic security measures on their personal computers if possible:

1. Install an antivirus program
   - Installing an antivirus program and keeping it up to date can help defend your computer against viruses. Antivirus programs scan for viruses trying to get into your email, operating system, or files. New viruses appear daily, so set your antivirus software to install updates automatically.
2. Use a firewall
   - A firewall can help alert you to suspicious activity if a virus or worm attempts to connect to your computer. It can also block viruses, worms, and hackers from attempting to download potentially harmful programs to your computer.
3. Keep your computer updated
   - Operating system and application security updates should be maintained in order to address vulnerabilities in the software.

Intentionally disabling any security mechanisms on District systems or intentionally infecting any system on The District network with malware is considered a form of vandalism and appropriate disciplinary measures will be taken.

5. Netiquette:

You are expected to abide by generally accepted rules of network etiquette (or netiquette). These include, but are not limited to, the following:

- Users shall not create or transmit harassing, threatening, abusive, defamatory or vulgar messages or materials.
- Illegal activities are strictly forbidden.
- Never reveal personally identifiable information like full name, address, phone number, etc. over the internet.
- Do not post names with personal pictures on the Internet. Information that has been posted on the Internet, it is likely posted and archived forever by Internet archiving sites such as http://www.archive.org.
- Unless you are registering for a service directly related to your coursework, do not register for anything on the World Wide Web, which involves filling out a form on The District network.
- District computers are used by multiple users throughout the day. Leave the computer in as good as or better shape than you found it.
- Do not use the network in such a way that you would disrupt the use of the network by other users.

6. Guarantee of Service:

The District makes no warranties of any kind, express or implied in connection with the service it is providing. The District will not be responsible for any damages, claims, losses, or cost of any kind (including attorneys fees) that users suffer which is in any way related to use of the District's technology or network. This includes loss of data resulting from delays, non-deliveries, erroneous deliveries or service interruptions caused by negligence, errors, or omissions. Use of any information obtained via The District's network is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. No assumption of privacy should be made when District personnel investigate problems with, or inappropriate use of any system.

Security on any computer system is a high priority, especially when the system involves many users. If you can identify a security problem on The District's network, you must notify the IT Department or a faculty member. Do not demonstrate the problem to others users. **Do not use another individual's account**. Attempts to login to the system with an account that does not belong to you will result in disciplinary action. Any user identified as a security risk or having a history of problems with other computer systems may be subject to disciplinary actions.

7. Vandalism:

Vandalism may result in disciplinary action, up to and including termination/expulsion, as well as financial responsibility to cover the cost of system recovery. Vandalism is to willfully harm or destroy data or any hardware/software associated with The District. If a device is issued to a student, any damage that is not consistent with normal wear and tear will be the responsibility of the student to whom the device was assigned.Copyright and Intellectual Property:

Students who use the intellectual property of others must pay attention to the portion limits and distribution allowed under the Laws of Fair Use; this includes citing the owner of the work. The District understands that work created by students is copyrighted to the respective individuals. The District also recognizes the importance of sharing quality work with wider audiences in order to either showcase or increase the quality of similar work. In this realm, The District seeks permission for the right to display student created materials to the public for the reasons stated above.

8. Student Assigned Devices:

- Students must take every reasonable precaution to prevent theft.
- Students must take precautions to prevent damage to District devices (i.e. keep devices away from liquids and extreme heat, transport devices in a protective case, do not leave devices where they will be crushed or dropped, etc.).
- Students will not install applications without the express permission of District administration. Students may not modify the configuration or circumvent security setting or Internet filtering.
- Devices may not be modified cosmetically: students will not write on the device or apply stickers to the device. Student may not remove District labels or asset tags from the device.
- Students will be responsible for adapters. Adapters will be registered and assigned with the device.

  Students will not trade adapters, and will endeavor to ensure the assigned adapter stays with the device. The adapter and power port are fragile; care must be taken when plugging in and unplugging the adapter. It is also important to keep cords where they will not be tripped on: tripping on a cord is likely to damage the device.
- Students will be charged a flat rate of $25.00 annually to cover the administration of the devices. In the event a device is non-intentionally damaged, a mandatory $15.00 deductible will be assessed per incident.

9. Personal Technology Tools:

Any technology tool, including but not limited to: handheld computers, cell phones, smart phones, laptops, tablets, still image and video cameras, recorders, and other assistive technology, whether used on or off The District's network, which are brought into District facilities must be used in accordance with Sections 1 through 9 above and may only be used to support the educational process.

These devices may only be used for work that directly corresponds to schoolwork during school hours. Games, Internet surfing, social networking, messaging, and recording are prohibited unless the activity is directly tied to the educational process. Any recordings or photographs capturing students, student work, or other school activity may be considered part of the student record, which is protected by The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) and may not be published or shared outside of the educational context. Failure to abide by these guidelines could result in the student losing privileges and/or disciplinary action up to and including expulsion.

Users are responsible for the condition and maintenance of their individual devices. The District does not assume responsibility for personal electronic devices that are lost or damaged. These devices are the property of the user and will be treated as such.

There must be a signed Student/Parent/Guardian Permission Form or Staff/Volunteer Agreement Form on file before the user gains access to the Network. Parents/Guardians will complete the Student/Parent/Guardian Permission Form upon registration for new students annually. The signed form will be kept in the student's cumulative folder. Employees will complete the Staff/Volunteer Agreement form upon employment. The signed form will be kept on record