

# Reynoldsburg City Schools

## Computer and Technology Acceptable Use Policy

Staff, Volunteers and Students



### *AUP Sections*

- |                                     |                                       |
|-------------------------------------|---------------------------------------|
| 1 – Acceptable Use                  | 6 – Guarantee of Service              |
| 2 – Privileges                      | 7 – Security                          |
| 3 – Internet and Information Access | 8 – Vandalism                         |
| 4 – Procedures & Caveats            | 9 – Copyright & Intellectual Property |
| 5 – Netiquette                      | 10 – Personal Technology Devices      |

*Reynoldsburg City School District offers a variety of technology tools and networked computer access to all students and staff. Many personally owned technology devices are being used to support and enhance the educational process too. 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 a responsibility on the part of the user 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. Due to the rapid change in technology, a user's access and/or this Policy are subject to change at any time. Each technology user (student and staff) will be held responsible for the following guidelines:*

### **1. Acceptable Use:**

Technology must be used to support education and research and be consistent with the objectives of Reynoldsburg City School 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 generally not acceptable. Use for any kind of product or service advertisement, or political lobbying is also prohibited.
- Installation of software, freeware, shareware, and demos not owned or authorized by the Reynoldsburg City School District is prohibited on district computers.
- Staff members are assigned a district e-mail account. The primary purpose of this account is to conduct **school** business. It is expected that all communication on this District owned forum is professional and school related. All communication in this District owned forum is subject to District review and public records request. Assume no right to privacy. Users routinely shall delete outdated or unnecessary e-mails from their mailboxes.
- Games are not considered an educational use of technology. Games may not be played when using technology tools within the Reynoldsburg City School District with the following exceptions:
  - Games that are created as part of an educational curriculum.
  - Games that directly support current curricular objectives.

### **2. Privileges:**

The use of the Reynoldsburg City School District Network is a privilege, not a right, and **inappropriate use may result in a cancellation of those privileges**. The district administrators, school administrators, teachers, and 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 Reynoldsburg City School District Network. The school disciplinary ladder and/or individual rules for specialized facilities will determine consequences.

Building Principals and Central Office Administrators may close an account at any time. The administrators, faculty, and staff of the Reynoldsburg City School District may request the Technology Department to deny, revoke, or suspend specific user rights and/or accounts. In a school environment such as the Reynoldsburg City School District, much of the work is produced on computers. Loss of privileges could have a very serious impact on academic opportunity and success of an individual.

### **3. Information and Internet Access:**

In compliance with the Federal Child Internet Protection Act (CIPA) the Reynoldsburg City School District filters the Internet for inappropriate content. All devices accessing the Internet through the District Network receive filtered Internet content.

#### **Filtered/Blocked Internet Sites:**

- Intolerance and Hate
- Criminal Activity
- Tasteless and Offensive
- Violence and Weapons
- Alcohol and Tobacco
- Illegal Drugs
- Gambling
- Hacking
- Spyware
- Proxies and Translators
- Phishing/ Fraud
- Personals, Dating, and Chat
- Intimate Apparel and Swimwear
- Non-educational Games
- Sexually Explicit Images
- Other Sites

It should be noted that, although Internet filters are very effective there is no such thing as a 100% perfect Internet filter technology. Be aware that it may be possible for an inappropriate website, particularly a new one, to pass through the filter. Students should simply close any webpage deemed inappropriate and tell a staff member what happened. Staff should, if possible, report the Internet address (URL) of the inappropriate site to the Technology Department by e-mail or submitting a Help Desk ticket.

With Internet access comes the responsibility to use this powerful educational tool wisely and in accordance with all other sections of this appropriate use policy. Purposeful intent to bypass or compromise the District Internet filter is considered inappropriate use. Random searching for information, which could be classified in the above examples of filtered categories, 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". E-mail used to transmit a document from home to school for educational purposes would be considered an appropriate use of this technology, however, instant messaging a friend to conduct friendly chat would not.

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. Generally, downloading published music or video without paying for it legitimately is illegal. Students and staff need to familiarize themselves with copyright and fair use laws and guidelines.

### **4. Procedures and Caveats:**

Files older than one year may be deleted at any time to make room for current project work. If you have older files you want to keep, you need to make a copy on a disk, thumb drive, or recordable DVD or CD-ROM. 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 technology team know so that proper arrangements can be made (provided sufficient storage space is available).

•Some large file types may be deleted immediately if no educational value is apparent. It is the user's responsibility to keep your 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.)**

•**Viruses and Other Malware** are an ongoing problem. Malware is a term used to describe any software program whose intentions are to destroy or disrupt a system. Although viruses are the most well known malware, worms and Trojan horses are the fastest growing category of malware today. 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 software on all district owned systems, spam and virus filtering software for the e-mail servers, strengthened security settings on systems, rapid deployment of security updates, and a firewall to protect the district network. Due to the increasing interconnectedness of computer networks it is in the district's best interests to ensure that personally owned technology devices such as home computers and notebooks are free of malware as well.

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

1. Install and regularly updated virus protection software.
2. Enable the a Firewall or use a third party firewall program.
3. Turn on Automatic Updates to automatically install security fixes.

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 your personal address, phone number, credit card number or those of other students or colleagues via Internet computer resources.
- 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 [www.archive.org](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:**

Reynoldsburg City School District makes no warranties of any kind for the service it is providing. Reynoldsburg City School District will not be responsible for any damages you suffer. 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 District Network is at your own risk. Reynoldsburg City School 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 on the District network.*

### **7. Security:**

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on Reynoldsburg City School District network, you must notify the Technology 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 as any other user will result in cancellation of user privileges. Attempts to login to the Reynoldsburg City Schools network or other school computing facilities as a system operator or administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to The Reynoldsburg City School District Network and/or other school computing facilities.

### **8. Vandalism:**

Vandalism may result in cancellation of network privileges as well as financial responsibility to cover the cost of system recovery. Vandalism is defined as any attempt to harm or destroy data or accounts of other users, or any hardware or software associated with Reynoldsburg City School District.

### **9. 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. Reynoldsburg City Schools understands that work created by students or staff is copyrighted to the respective individuals. The district also recognizes the importance of sharing quality work with wider audiences in order to either showcase the work or increase the quality of similar work. In this realm, the district seeks permission for the right to display student and staff created materials to the public for the reasons stated above.

### **10. Personal Technology Tools:**

Any technology tool such as handheld computers, cell phones, smart phones, laptop computers, tablets, still and video cameras, recorders, and other assistive technology, whether used on or off the District 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, and messaging are prohibited unless the activity is directly tied to school activities. Failure to abide by these guidelines could result in the student losing privileges and benefits of using these technologies during school hours. Students are responsible for the condition and maintenance of their individual devices. Reynoldsburg City School District does not assume responsibility for personal electronic devices that are lost or damaged. These devices are the property of the student 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 in the employee's personnel file.***



**Reynoldsburg City Schools**  
Computer and Technology Acceptable Use Agreement  
**Staff and Volunteers**



**All Board policies are available in each school's administrative office and on the district website.**

I have read, understand and agree to abide by the Network Acceptable Use Policy. I agree to report any misuse of the technology to the building principal or central office technology department and to cooperate in any investigations regarding security issues and/or improper or illegal uses of the technology. I understand that my technology account may be monitored. I agree to exercise responsibility by using my best efforts not to violate this Policy.

I understand that any violation of this Policy may subject me to restriction, termination of my access to district technology, formal disciplinary action in accordance with the staff contract and other Board policies, referral to legal authorities, and/or other legal action, and possible termination of employment.

By signing below, I agree to release Reynoldsburg City School District, its administrators, teachers, employees and Board members, from any claims or damages arising as a result of and in connection with my failure to follow school policies regarding use of the Network, including claims or damages arising from the staff member or volunteer giving his/her user name or password to another individual.

\_\_\_\_\_  
Staff/Volunteer Name (Printed)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date