**ReynoldsburgCitySchools**

Computer and TechnologyAcceptableUse Policy Staff,VolunteersandStudents

AUP Sections

1. Acceptable Use 2. Privileges

3. Internet Access

4. Procedures & Caveats

5. Netiquette

6. Guarantee of Service 7. Vandalism

8. Copyright & Intellectual Property 9. Student Assigned Devices

10. Personal Technology Devices

The Reynoldsburg City School District (“The District”) offers a variety of technology tools and networked computeraccess to allcurrentlyenrolledstudents andstaff (“user(s)”). Manypersonallyowned devices are being used to support and enhancethe educationalprocess. These resources anddevices, whether District ownedor 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 technologyor 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 compliancewiththe following guidelines:

**1.** **AcceptableUse:**

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 electroniccommunication.

• Transmissionof anymaterialinviolationof anyfederalorstateregulationisprohibited.This includes, but is not limited to: copyrighted material, threatening, harassing, or obscene material, or material protectedbytradesecret.

• Use for commercial activities by for-profit institutions is prohibited. Use for any kind of product or serviceadvertisement,orpolitical lobbyingisalsoprohibited.

• Installationof softwarenotownedorauthorizedbyThe DistrictisprohibitedonDistrictcomputers.

• 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 systemis 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. Assumenoright 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/appssuchasGoogle HangoutsMeet, 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 technologytools withinTheDistrictwiththefollowingexceptions:

 Games that arecreatedas partof an educational curriculum.

1

*Reynoldsburg* *City* *School* *District*

 Gamesthatdirectlysupportcurrentcurricularobjectives. **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.** **InformationandInternetAccess:**

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 Internetcontent. Districtowneddevices,evenifusedoffsite,willonlyaccesstheInternetthroughaDistrict 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 thatareobscene, childpornography,orharmfultominors."

AlthoughInternetfiltersareveryeffective,thereis nosuchthingas 100% perfectInternetfiltertechnology. 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 shouldreporttheInternet address (URL) of theinappropriatesitetotheIT Department by e-mailor submittinga Help Deskticket.

TheInternetispowerfuleducationaltool.IndividualsareresponsibleforInternetusageinaccordancewith allsectionsofthisAcceptableUsePolicy(AUP).WillfulintenttobypassorcompromiseTheDistrictInternet filter isconsideredinappropriateuse. Randomsearching for informationwhichcouldresult in the display of content that is obscene or harmful to minors,is inappropriate use. Bringingcontentinto theDistrictthat would otherwise be filtered is also considered inappropriate. In addition, specific Internet sites may be added toor removedfromthe “Block List”.

A critical part of using the Internet as a resource is for the user to learn how to determine the validity of informationposted.Downloading informationfromtheInternet shouldbe done with caution. Just because it is posted, does not mean it is legal to download. Downloading media protected by copyright without payingforit legitimatelyis illegal.Students andstaff needtofamiliarizethemselves with copyrightandfair uselawsand guidelines (see section 8 of this AUP). Copyright violation is illegal, and in accordance with this policy is strictlyprohibited.

**4.** **ProceduresandCaveats:**

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 storagelocation.If youneedtokeepanumberof largefilesforanextendedperiodoftimeonschool equipment, please let a member of theIT Department knowso that arrangements canbe 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 educationalvalueisapparent. Itistheuser’sresponsibilitytokeepfoldersfreeoffilesforwhichthereexists nofurtheruse.

**These** **mayinclude,** **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.)**

2

*Reynoldsburg* *City* *School* *District*

**Viruses** **andMalware:**

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 measuresinclude,butarenotlimitedto:virusprotection,behaviormonitoring,network threat inspection, spam filtering, bolstered security settings, rapid deployment of security updates, and a firewall to protect The District’s network fromexternal 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** **securitymeasuresontheirpersonalcomputersifpossible:**

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

 Operatingsystemandapplicationsecurityupdates shouldbemaintainedinordertoaddress 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:**

Youareexpectedtoabidebygenerallyacceptedrulesofnetwork etiquette(ornetiquette).Theseinclude, 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 strictlyforbidden.

 Never reveal personally identifiable information likefull 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.](http://www.archive.org/)

 Unless you are registering for a service directly related to your coursework, do not register for anything on theWorldWide Web, which involves filling out a form on The District network.

 Districtcomputersareused bymultipleusersthroughouttheday.Leavethecomputer inasgood 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.** **GuaranteeofService:**

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 serviceinterruptions causedbynegligence,errors,oromissions.Useof anyinformationobtained via The District’s network is at your own risk. The Districtspecificallydenies any responsibilityfor 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.

3

*Reynoldsburg* *City* *School* *District*

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:**

Vandalismmay resultin disciplinaryaction, up to and including termination/expulsion,as wellas 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, anydamage that is not consistent with normal wear and tear will be the responsibility of the student to whom the device was assigned.CopyrightandIntellectualProperty:

Students whousetheintellectual propertyof othersmustpayattentiontotheportionlimitsanddistribution allowed under the Laws of Fair Use; this includes citing the owner of the work. The District understands that work createdbystudents is copyrightedto therespective individuals. The Districtalsorecognizes the importanceof sharingqualityworkwithwideraudiencesinordertoeithershowcaseorincreasethequality 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** **AssignedDevices:**

 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.PersonalTechnologyTools:** Anytechnologytool,includingbutnotlimitedto:handheldcomputers,cellphones,smartphones, 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 directlytied 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.

4

*Reynoldsburg* *City* *School* *District*

**TheremustbeasignedStudent/Parent/GuardianPermissionFormorStaff/Volunteer** **AgreementForm** **onfile** **beforethe** **usergainsaccess** **totheNetwork.** **Parents/Guardians** **willcompletetheStudent/Parent/GuardianPermissionFormupon** **registrationfornew** **students** **annually.Thesigned** **formwillbekeptin** **the** **student’s** **cumulative** **folder.** **EmployeeswillcompletetheStaff/Volunteer** **Agreementformupon** **employment.The** **signedformwillbekept** **on** **record**

5

*Reynoldsburg* *City* *School* *District*

**Reynoldsburg** **CitySchools** Technology Acceptable Use Agreement **Students/Parents/Guardians**

**AllBoardpolicies** **areavailableineach** **school’s** **administrativeoffice** **andon** **reyn.org.**

I have read, understand and agree to abide bythe ComputerTechnology Acceptable Use Policy. I agree to report any violation of this policy to the building principal or IT Department and to cooperate in any investigations regarding violations. I understand that mytechnologyaccount maybe monitored. I agree to exercise responsibilitybyusingmybest efforts notto violate this policy.

I understand that anyviolation of this Policymaysubject me to restriction or termination of my access to district technology, discipline in accordance with the student handbook, other Board policies, referral to legal authorities, and/orother legalaction.

Bysigning below, I agree to release The Reynoldsburg City School District Board of Education, its staff and Board members, from anyclaims or damages arising as a result of or in connection with myuse of District technology or the District’s network, including claims or damages arising from the use of same bysomeonetowhomIhavegivenmyusernameorpassword.

Student Name (Printed) Student Signature Date

***If*** ***the*** ***student*** ***named*** ***aboveis*** ***under*** ***18*** ***years*** ***of*** ***age,*** ***a*** ***parent*** ***or*** ***legal*** ***guardian*** ***must*** ***completethefollowing:***

**PARENT/GUARDIANPERMISSIONFORM**

I have read and understand the District’s Computer and Technology Acceptable Use Policy, and agree to its terms. As a parent or legal guardian of the minor student signing above, I grant permission for my daughter/son/wardtoaccessDistricttechnologyresources,includingnetworkedcomputer servicessuch as the Internet. I understand that some accessible materials may be objectionable, and I accept responsibility for setting and conveying standards for my daughter/son/ward to follow when selecting, sharing,or exploringinformationandmedia.

By signing below, I agree to release The Reynoldsburg City School District Board of Education, its staff and Board members, from any claims or damages arising as a result of or in connection with my child’s/ward’s use of the Network or District technology, including claims or damages arising from my child giving his/her user name or password to another person. I am aware of and agree to the $25.00 annual charge to cover the administration of devices (this only applies to devices assigned to be taken home bystudents), and a $15.00 deductible per incident if the device is non-intentionally damaged.

Parent/Guardian Signature

Home Phone #

Work Phone #

Date

Student ID #

Student Dateof Birth

6

*Reynoldsburg* *City* *School* *District*

**Reynoldsburg** **CitySchools** Technology Acceptable Use Agreement **Staff** **and** **Volunteers**

**AllBoardpolicies** **areavailableineach** **school’s** **administrativeoffice** **andon** **reyn.org.**

I have read, understand and agree to abide by the Computer andTechnology Acceptable Use Policy. I agree to report anymisuse of technologyto the building principal or IT Department and to cooperate in anyinvestigation(s)regardingsecurityissuesand/orimproperorillegaluse oftechnology.I understand thatmytechnologyaccountmaybemonitored.Iagreetoexerciseresponsibilityby usingmybestefforts notto violate this policy.

I understand that any violation of this policymaysubject me to restriction, termination of my access to Districttechnologyresources,formaldisciplinaryaction (inaccordance withthestaff contractand other Board policies) up to and including termination of employment,referralto legalauthorities,and/orother legal action.

Bysigningbelow, Iagreeto release TheReynoldsburg CitySchoolDistrict Board of Education, itsstaff and Board members, from anyclaims or damages arising as a result of or inconnection withmy use of District technology or the District’s network ,including claimsordamagesarisingfrom the use of same by someone to whom I have given my usernameor password.

Staff/Volunteer Name (Clearly Printed) Signature Date

Job Title SchoolWher**e** Staff/VolunteerWill be Located

Contact Informationfor Staff/Volunteer

*Please* *List* *an* *Email* *Address* *&* *or* *Phone* *Number* *Where* *the* *IT* *Dept.* *Can* *Securely* *Relay* *Your* *Username* *and* *Password*

7

*Reynoldsburg* *City* *School* *District*