

# Johnson City Schools Technology Acceptable Usage Agreement

## **Mission:**

The mission of the Johnson City Schools is to enable all students to achieve excellence in learning, social responsibility, and self-worth.

## **Scope of Use:**

To ensure that students receive a quality education in an intellectually stimulating environment, it is the goal of the Johnson City Schools to provide all students with access to a variety of technological resources.

The creation of a large and varied technological environment demands that technology usage be conducted in legally and ethically appropriate ways consistent with the policies and instructional goals of the Johnson City Schools.

Thus, it is the intention of the Johnson City Schools that all technological resources be used in accordance with any and all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is understood that all students and employees of Johnson City Schools will use the provided technological resources so as not to waste or abuse, interfere with or cause harm to other individuals, institutions, or companies.

## **Rules for Usage:**

The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of the Johnson City Schools. Use of any and all technological resources is a privilege and not a right. Any violation of the Acceptable Usage Agreement may result in termination of usage and/or appropriate discipline. **All Johnson City Schools students and their parent/guardians and all Johnson City Schools employees must sign this agreement as acknowledgment of receipt of these procedures and policies.**

### **I. ACCESS:**

- A. Any student or employee who accesses the district's network or any device for any purpose agrees to be bound by the terms of the Agreement, even if no signed Agreement is on file.
- B. The use of all Johnson City Schools technological resources is a privilege, not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges pending investigation.
- C. Access to the Internet by students by any means other than the District's network while in a Johnson City School facility is prohibited.
- D. Except at approved locations or as otherwise approved, all devices connected to the Johnson City Schools physical network (a device located at a Johnson City School facility, either wired or wireless) must be the property of Johnson City Schools. Individuals connecting a personal device to the Johnson City School's network will be required to agree to stated Terms and Conditions and log in with

system provided account information. Individuals may use only accounts, files, software, and technological resources that are assigned to him/her.

- E. Individuals may not log in to or attempt to log in to the network by using another person's account and/or password or allow any other person to use his/her password to access the network, e-mail, or the Internet.
- F. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and/or outside the Johnson City Schools.
- H. Individuals identified as a security risk may be denied access to the District's technological resources.
- I. Any use of technological resources that reduces the efficiency of use for others will be considered a violation of this agreement.
- J. Individuals must not disrupt or attempt to disrupt any computer services or data by spreading viruses, spamming or by any other means.
- K. Individuals must not modify or attempt to modify hardware, utilities, and configurations, or change the restrictions associated with his/her accounts, or attempt to breach any security system, either with or without malicious intent.
- L. The District Technology Coordinator and/or site administrators will determine when inappropriate use has occurred and each has the right to deny, revoke, or suspend specific user accounts and access. Users have the right to appeal the decision to the site administrator or Superintendent of Schools.

## **II. PRIVACY:**

- A. To maintain network integrity and to ensure the network is being used responsibly, the District Technology Coordinator reserves the right to review files and network communications.
- B. Users should have no expectation of privacy with regards to any data stored, transmitted or accessed on school system resources.
- C. Because communications on the Internet are often public in nature, all users should be careful to maintain appropriate and responsible communications.
- D. The Johnson City Schools cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.
- E. All computer hardware and software belongs to the school system. All data including search histories and email communications transmitted on school system computers or by means of the school system network are subject to monitoring and may be archived.
- F. Users are encouraged to avoid storing personal and/or private information on the district and/or schools technological resources.
- G. The system-wide technology staff performs routine backups. However, all users are responsible for the backup and storage of any critical files and/or data.

## **III. COPYRIGHT:**

- A. Illegal copies of software may not be created or used on school system equipment.
- B. Any questions about copyright provisions should be directed to the District Technology Coordinator.

- C. The legal and ethical practices of appropriate use of technological resources will be taught to all students in the system (i.e. during lab orientation, network orientation, etc).
- D. Copyright is implied for all information (text, data, and graphics) published on the Internet. Users are prohibited from the reproduction or use of works, including but not limited to documents, pictures, digital recordings, music or graphics, without documented permission.
- E. Duplication of any copyrighted software is prohibited unless specifically allowed for in the license agreement and then should occur only under the supervision and direction of the Technology department. This includes duplicating original music CD's.
- F. A backup copy of all purchased software programs should be made and thus become the working copy.
- G. All original copies of software programs including those purchased with departmental funds will be stored in a secure place.
- H. For security and insurance purposes, the District Technology Coordinator or site administrators will be the only people with access to original software disks at a given location with the exception of CD-ROMs. System-wide software originals will be housed at the district Technology Coordinator's office.
- I. If a single copy of any given software package is purchased, it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk onto multiple computers," (1987 Statement on Software Copyright) is NOT allowed.
- J. If more than one copy of a software package is needed, a site license, lab pack, or network version must be purchased. The District Technology Coordinator and the person requesting the software will be responsible for determining how many copies should be purchased.
- K. Either the district Technology Coordinator or site administrator at each location is authorized to sign license agreements for a site within the system. Copies of any system-wide license agreements must be signed by the District Technology Coordinator and/or Superintendent and distributed to all schools that will use the software.
- L. The District Technology staff or site technology assistant is responsible for installation of all software in use on the local area network and/or individual workstations within the Johnson City Schools.
- M. Users should not purchase software for use on District computers or other technological resources without prior consultation with the District Technology staff.

#### **IV. ELECTRONIC MAIL:**

- A. Johnson City Schools may provide access to electronic mail for students in grades 7-12. Access to instant messaging will not be provided for students. Use of email on school system resources or personal devices used during the school day shall be limited to the school provided email account. Students with network access may not utilize school system resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system.

- B. The Johnson City Schools does provide access to electronic mail for all employees.
- C. Access to e-mail is for employee/student use in educational and instructional settings.
- D. Personal use of electronic mail for employees is permitted as long as it does not violate Johnson City Schools' policy and/or adversely affect others or the speed of the network.
- E. Electronic mail should reflect professional standards at all time.
- F. Johnson City Schools' e-mail accounts may not be used for political or personal gain.
- G. All data, including e-mail communications, stored or transmitted on school system devices shall be monitored. Johnson City Schools' e-mail accounts may not be used for sending or attempting to send anonymous messages.
- H. Johnson City Schools' e-mail accounts may not be used for sending mass emails.
- I. Johnson City Schools' e-mail accounts may not be used for posting or forwarding other user's personal communication without the author's consent.
- J. E-mail correspondence may be a public record under the public records law and may be subject to public inspection.
- K. Instant messaging is prohibited.

#### **V. INTERNET:**

- A. The intent of the Johnson City Schools is to provide access to resources available via the Internet with the understanding that faculty, staff, and students will access and use information that is appropriate for his/her various curricula.
- B. All school rules and guidelines for appropriate technology usage shall apply to usage of the Internet.
- C. Teachers will screen all Internet resources that will be used in the classroom prior to their introduction.
- D. Students will gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from parents/guardians via this signed agreement.
- E. Students will be allowed to conduct independent research on the Internet upon the receipt of the appropriate permission forms.
- F. Permission is not transferable, and therefore, may not be shared.
- G. Students that are allowed independent access to the Internet will have the capability of accessing material that has not been screened.
- H. Students at approved locations may use personal devices to access the Internet as long as access is gained via the school systems network and only at the discretion of their teacher during class time.

#### **VI. INTERNET FILTERING:**

- A. Internet access for all users is filtered by a filtering system through one central point, by URL and IP address.
- B. Internet searches are filtered by keyword.
- C. URLs and IP addresses may be added to or deleted from the filtered list by the District Technology staff.
- D. Employees may request a review for override of filtered sites.

## **VII. INTERNET SAFETY MEASURES**

- A. Internet safety measures shall be implemented that effectively address the following:
  - 1. Controlling access by students to inappropriate matter on the Internet.
  - 2. Safety and security of students when using any form of direct electronic communications;
  - 3. Preventing unauthorized access, including “hacking” and other unlawful activities by students on-line; and
  - 4. Restricting students’ access to materials that may be inappropriate or harmful to them.
- B. The processes for ensuring that the system’s resources are not used for purposes prohibited by law or for accessing sexually explicit material are:
  - 1. Monitoring on-line activities of students;
  - 2. Utilizing technology that blocks or filters Internet access (for both students and adults) to material that is obscene, pornographic or potentially harmful to students; and
  - 3. Maintaining a usage log.
- C. All students will participate in Internet safety training, which is integrated into the District’s instructional program in grades K-12. Schools will use existing avenues of communication to inform parents, grandparents, caregivers, community stakeholders and other interested parties about Internet safety.
- D. The District’s Internet Safety Policy and the Technology Acceptable Usage Agreement shall be reviewed, evaluated and revised, as needed, annually.

## **VIII. WEB PUBLISHING:**

- A. The Johnson City Schools' web server cannot be used for profit, commercial purposes, to express personal opinions, or to editorialize.
- B. All web sites will be reviewed by the District Technology Coordinator or Principal before being added to the Johnson City School’s web server.
- C. The District Technology staff reserve the right to reject all or part of a proposed web page.
- D. Web pages may only be placed on the web server by the District Technology Coordinator or district Webmaster.
- E. All pages posted on the Johnson City Schools’ web server must be written with an approved editor.
- F. Each posted page must include: the school location, date of last update, and an e-mail address.
- G. All posted work must be of publishable quality with regard to spelling, usage, and mechanics.
- H. All web page authors are responsible for the maintenance of their own pages.
- I. All links should be checked regularly to make sure they are current and working.
- J. Pages that are not updated in a timely fashion, contain inaccurate or inappropriate information, or contain links that do not work will be removed and the author will be notified.
- K. Unfinished pages will not be posted until they are fully functional.

- L. Teacher created web pages stored on a commercial or private server may be a link from a school created web page stored on the Johnson City Schools' web server.
- M. Student pictures and other personally identifiable information should only be used with permission in writing from the parent/guardian of the student involved. No full names should be used-only first name, last initial. No written permission is required for in-school broadcasts (i.e. morning news, announcements, class profiles, etc.)
- N. Student posting of personal information about himself/herself or other students or staff of any kind is prohibited. Personal information includes: home and/or school address, work address, home, cellular and/or school phone numbers, full name, social security number, etc.
- O. No written permission is required to list faculty/staff and their school contact information (phone extension, e-mail address, etc.)
- P. Consent will be required for posting of any employee photographs.
- Q. Infringement of copyright laws and the posting of obscene, pornographic, harassing or threatening materials on web sites are against the law and will subject the responsible party to discipline and/or prosecution.

#### **IX. PROHIBITED USES:**

The following activities are examples of inappropriate activities on any Johnson City Schools network, e-mail system, or the Internet. This list is not all-inclusive. Anything that would be considered inappropriate in "paper form" is also considered inappropriate in electronic form.

- A. Using another user's password or attempting to find another user's password.
- B. Sharing your own password.
- C. Trespassing in another user's files, folders, home directory or work.
- D. Saving information on ANY network drive or directory other than your personal home directory or a student specified and approved location.
- E. Downloading, installing, or copying software of any kind onto a workstation, your home directory, or any network drive.
- F. Harassing, insulting, threatening, bullying or attacking others via technological resources.
- G. Damaging computers, computer systems, or computer networks (this includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.)
- H. Intentionally wasting limited resources such as disk space and printing capacity.
- I. Accessing inappropriate web sites (sites containing information that is violent, illegal, sexually explicit, racist, etc.)
- J. Sending, displaying, or downloading offensive messages or pictures.
- K. Using obscene, racist, profane, lewd, discriminatory, threatening, or inflammatory language.
- L. Participating in on-line chat rooms or the use of instant messaging without the permission/supervision of an adult staff member.
- M. Posting any false, damaging or libelous information about other people, the school system or other organizations.

- N. Posting any personal information about another person without his/her written consent.
- O. Impersonating another individual.
- P. Broadcasting network messages and/or participating in sending/perpetuating chain letters.
- Q. Violating copyright laws.
- R. Plagiarism of materials.
- S. Use of technological resources to create illegal materials (i.e. counterfeit money, fake identification, etc.)
- T. Use of any Johnson City Schools' technological resources for personal gain, commercial or political purposes.
- U. Use of Johnson City Schools' technological resources for purposes of hacking into other local area networks or outside networks.
- V. File-sharing or downloading file-sharing programs.
- W. Participating in any other activity that is detrimental to students, the school, the School District or school employees or officials.
- X. Attempting to bypass or bypassing the District's filtering system.
- Y. Accessing the Internet via a network other than the District's network, including access on personal devices.

### **Liability:**

The Johnson City Schools does not guarantee the reliability of the data connection and does not verify the accuracy of information found on the Internet.

### **Disciplinary Actions for Violation of Agreement:**

As a result of violating this agreement, below is a list of possible disciplinary actions:

- Sending a warning reminder to parent and student about the AUP agreement
- Loss of Internet privileges for one week
- Loss of Internet privileges for one month
- Permanent loss of Internet privileges
- Other disciplinary action to be determined by school administration

### **Appeal Process:**

An individual whose rights have been restricted or revoked has the right to appeal to the site administrator and the Superintendent of Schools.