



Guidelines for Acceptable Use of Technology Resources Richardson Independent School District

The Richardson Independent School District's vision is to provide an environment where all students learn, grow, and succeed, and its mission is to serve and prepare all students for their global futures. In support of those objectives, the District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the District's schools by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. All students and staff must take responsibility for the appropriate use and care of all technology resources they use. Access to and the use of these technology resources is a privilege, not a right.

While RISD has developed these acceptable use guidelines and provides training to encourage responsible use of technology resources, access to computers and the worldwide internet creates the possibility that material may be obtained that may not be considered to be of educational value in the school setting. RISD believes that the value of information, interaction, and research capabilities outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District.

Appropriate behavior, as it relates to the use of computers, is no different than appropriate behavior in all other aspects of RISD activities. Persons who access District technology resources, herein referred to as **users**, must use the computers and computer networks at all times in a responsible, ethical, and polite manner. This document is intended to clarify the District's expectations for the use of computer and network resources, and is consistent with RISD policy.

Definition of District Technology Resources

The District's computer systems and networks include any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This term includes electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The District reserves the right to and intends to periodically monitor and review all activities connected with the use of any District owned or provided technology resource. No user should have an expectation of privacy of any information on District owned or provided technology resources.

The District's Electronic Communication and Data Management Policy states that access to the District's electronic communication and data management systems will be provided to those persons who agree to comply with this Acceptable Use Plan (AUP) [See CQ (LOCAL) – Electronic Communication and Data Management Policy].

Employee access to the District's system will be granted with the written approval of the immediate supervisor if the employee has met the conditions of system access.

Students will be granted access to the District's system by the system administrator or a local building designee as appropriate. Students will be assigned individual accounts, where applicable.

The District may deny system access to any system user who (i) is identified as a security risk, or (ii) had violated the District's Electronic Communication and Data Management Policy or AUP. Other appropriate disciplinary action, as described in the policy and regulations, may also be assigned.

Acceptable Use

RISD technology resources shall be used only for learning, teaching and administrative purposes consistent with the District's vision. Commercial use of the District's system is strictly prohibited. Limited use of the system for personal communication is acceptable as long as it does not burden the system or interfere with the users' educational or employment responsibilities.

The campus will make training available to all users in the proper use of the system. A copy of the Acceptable Use Guidelines is available in both the RISD Student Code of Conduct and the Employee Handbook. A copy is also available online at www.risd.org. All training in the use of the District's system will emphasize the ethical use of this resource.

Software or external data may not be placed on any computer, whether stand-alone or networked to the District's system, without permission.

Other issues applicable to acceptable use are:

1. Copyright: All users are expected to follow existing copyright laws. RISD has designated an agent to receive notifications of alleged copyright infringement. If you believe your copyrighted work is being infringed on an RISD site, please notify the Executive Director of Instructional Technology.
2. Supervision and permission: A staff member only allows student use of the computers and computer network when supervised or granted permission.
3. Attempting to log on or logging on to a computer or email system by using another's password is prohibited. Assisting others in violating this rule by sharing information or passwords is unacceptable.
4. Attempting to bypass the district's communication system through the use of software or outside proxy systems is prohibited. Assisting others in violating this rule by sharing information or passwords is unacceptable.
5. Improper use of any computer or the network is prohibited. This prohibition includes, without limitation:
 - Submitting, publishing, or displaying any information, material, or image, either publicly or privately, to any person (teachers, students, parents, or other individuals or groups) that is defamatory, inaccurate, racially, sexually, or

religiously offensive, abusive, obscene, profane, sexually-oriented, or threatening.

- Using the network for financial gain, political, or commercial activity.
- Attempting to harm or harming equipment, materials, or data.
- Attempting to send or sending anonymous messages of any kind.
- Using the network to access inappropriate material.
- Knowingly placing a computer virus on a computer or the network.
- Using the network to provide addresses or other personal information that others may use inappropriately.
- Accessing of information resources, files, and documents of another user without authorization.

6. The user in whose name a system account is issued will be responsible at all times for its proper use.
7. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District guidelines.
8. Users may not use another person's system account.
9. Users, if granted access to electronic mail, must archive or delete electronic mail consistent with the District's retention policies.
10. Users should delete unneeded files from the District servers on a regular basis.
11. Users will be responsible for the care and maintenance of their systems. Maintenance issues should be reported to the campus computer facilitator.
12. Podcasts are allowed as long as:
 - The podcast is student or teacher created and is in support of district goals and/or supports the RISD approved curriculum.
 - The podcast is loaded on a District server or District approved podcast resource.
 - The content is appropriate under these guidelines and applicable District policies.
13. Blogs, Forums, Wikis and Personal Learning Networks are allowed as long as:
 - The postings are student or teacher created, and are in support of District goals and/or the RISD approved curriculum.
 - The postings are posted to a District server or approved District resource.
 - The content is appropriate under these guidelines and applicable District policies.
14. Streaming Video is allowed as long as:
 - The streaming video is in support of District goals and/or supports the RISD approved curriculum.

- The streaming video is student or teacher created and is in support of District goals and/or supports the RISD approved curriculum.
- The streaming video created by students or teachers is loaded on a District server or approved District resource.
- The content is appropriate under these guidelines and applicable District policies.

15. Online Applications use is allowed as long as:

- The online application is in support of District goals and/or supports the RISD approved curriculum.
- The online application is listed on the approved RISD resource list.
- Online application products are student or teacher created, and are in support of District goals and/or supports the RISD approved curriculum.
- The content is appropriate under these guidelines and applicable District policies.

Vandalism Prohibited

Any attempt to harm or destroy RISD equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited.

Forgery Prohibited

Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

Network Etiquette

System users are expected to observe the following network etiquette (also known as netiquette):

1. Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
2. Pretending to be someone else when sending or receiving messages is prohibited.
3. Submitting, publishing, or displaying any information, material, or image, either publicly or privately, to any person (teachers, students, parents, or other individuals or groups) that is defamatory, inaccurate, racially, sexually, or religiously offensive, abusive, obscene, profane, sexually-oriented, or threatening is prohibited.
4. Revealing such personal information as addresses or phone numbers of users or others is prohibited.
5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

6. Be polite. For example, messages typed in capital letters are the computer equivalent of shouting and are considered rude.

System Access

Access to the District's network systems for all users will be governed as follows:

1. Any system user identified as a security risk or having violated the Acceptable Use Policy will be denied access to the District's system. Other consequences may also be assigned.
2. Any system user having been denied access rights may be reinstated with a limited access account to reduce the level of security risk to the system. Limits on this type of account may include time limitations, station access limitations, file access restrictions, and a revocation of Internet access privileges.

Information Content / Third Party Supplied Information

Students and parents of students who are granted access to the District's system should be aware that use of the system may inadvertently provide access to other electronic communications systems outside the District's networks that may contain inaccurate and/or objectionable material. RISD maintains an Internet filtering software package to attempt to minimize the access to objectionable material. Any attempt to circumvent the filtering software will be viewed as an attempt to disrupt the system.

A user bringing prohibited materials into the District's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action.

Termination or Revocation of System User Account

Termination of an employee's or student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of the user's withdrawal or revocation of system privileges, or on a future date if so specified in the notice.

Disclaimer

The District's system is provided on an "as is, as available" basis. RISD makes no warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District.

RISD shall not be liable for users' inappropriate use of electronic communications resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs

incurred by users. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's technology resources.

Parents and guardians must be aware that while at school direct supervision is not always possible. The District will make reasonable attempts to limit access, but cannot guarantee that system users will not be able to access or create inappropriate material that is prohibited by the District's Electronic Communication and Data Management Policy. Therefore, students are expected to use the resources in a manner consistent with administrative regulations, guidelines, and user agreements and will be held responsible for their use. Additionally, parents should discuss with their children their own expectations for their child's use of technology resources.