Computer, Electronic Communications Systems, and Network Access

Acceptable Use Policy for Students and Employees

For

Royse City Independent School District Technology Resources

The Royse City Independent School District (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. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Royse City ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District. Royse City ISD complies with Federal Regulations regarding Internet filtering in order to limit user access to inappropriate content.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Royse City ISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, professional, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District policy.

Definition of District Technology Resources

The District's computer system and networks are defined as any configuration of computer hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, video, and audio files, and data files. This includes but is not limited to electronic mail, local databases, externally accessed databases (i.e. accessed via the Internet), CD-ROM or any storage device, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available (including handheld devices such as PDAs, smart phones, net books, web cameras, etc.). The District will, at its own discretion, monitor any technology resource activity without further notice to the end user.

Acceptable Use

The District's technology resources will be used only for learning, teaching, and administrative purposes consistent with the District's mission and goals. The District e-mail system should not be used for mass mailings except for official school business. Commercial use of the District's system is strictly prohibited except where designated by policy, for example the Gold Sheet. Personal e-mail should not impede the conduct of District business; only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the school day—should be used to attend to personal matters. Employee time may be restricted by the campus administrator.

The District will make training available to all users in the proper use of the system and will make copies of acceptable use guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource.

Software may only be installed on a district-owned computer, whether stand-alone or networked to the District's system, if purchased using RCISD monies. Only personnel authorized by the RCISD Technology Department may install software on any computer. Proof of purchase will be required before installation of software can take place.

Other issues applicable to acceptable use are:

1. ***Copyright:*** All users are expected to follow existing copyright laws, copies of which may be found in each campus library.
2. ***Supervision and permission:*** A student may use a computer only if supervised and granted permission by a RCISD staff member.
3. ***Attempting to log on or logging on to a computer or e-mail system by using another's password is prohibited:*** Assisting others in violating this rule by sharing information or passwords is a violation of RCISD policy.
4. ***Improper use of any RCISD computer or the network is prohibited. This includes but is not limited to the following:***
    - Submitting, sending, posting, publishing, printing, forwarding or intentionally displaying any information that is defamatory, purposely inaccurate, racially or religiously offensive, abusive, discriminatory, bullying, obscene, profane, sexually oriented, harassing, threatening, damaging to another's reputation, or illegal
    - Using the network for financial gain, political or commercial activity except where preapproved and appropriate (instructional projects, Gold Sheet, payment of accounts, etc.)
    - Attempting to or harming RCISD equipment, materials, or data
    - Attempting to or sending anonymous messages of any kind from a RCISD computer
    - Using the network to intentionally access inappropriate material
    - Knowingly placing or installing a computer virus or any other destructive computer code on a RCISD 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
    - Using a network account belonging to someone else

- By-passing RCISD proxy servers
- Posting personal information about others without proper authorization
- Downloading or using unlicensed copyrighted material without a legitimate claim of fair use.
- Attempting to "hack" into network resources
- Storing inappropriate information (e.g., .jpeg and .exe files) in home directories or shared files
- Unauthorized access of the RCISD grade book or any RCISD student data system
- Disabling or attempting to disable any RCISD Internet filtering device
- Encrypting communication through the RCISD network to avoid security review
- Wasting school resources through the improper use of the computer system
- Gaining unauthorized access to restricted RCISD information or resources
- Personal printers, scanners or computers attached to the RCISD system
- Unless part of the approved RCISD curriculum, the following rules also apply:
    - Students are prohibited from changing any computer settings and/or configurations
    - Students may not install any software, including but not limited to commercial software, shareware, freeware, original software, plugins and/or utilities onto school computers or networks
    - Students are not allowed to open computer cases (CPU's) or make modifications to computers

System Access

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

1. RCISD student users will have access to the District's resources for class assignments and research with their teacher's permission and supervision.
2. Teachers with accounts will be required to maintain password confidentiality by not sharing passwords with anyone.
3. Teachers are not allowed to provide student access through the teacher's account.
4. Any system user identified as a security risk or having violated District Acceptable Use Policies may be denied access to the District's system. Other consequences may also be imposed (see Consequences of Improper Use)
5. 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 limitation, home directory limitation, station access limitations, file access restriction, and revocation of Internet access privileges.

Campus Level Responsibilities

The campus principal or designee will:

1. Be responsible for disseminating and collecting signed permission forms, and enforcing the District Acceptable Use Policy for the District's system at the campus level.
2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

Individual User Responsibilities

The following standards will apply to all users of the District's computer network systems:

1. The individual in whose name a system account is issued will be responsible for its proper use at all times.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policies.
3. System users may not use another person's system account to access computer or network resources.
4. System users are required to delete outdated electronic mail or files on a regular basis. Before deletion, users must determine if the contents of the email or file require retention under the state records retention regulations.
5. System users will be responsible for the care of their systems. Maintenance issues must be reported to the Campus Technology Assistant, helpdesk, or technology coordinator in a timely manner.
6. System users will be responsible for following all copyright laws.

Vandalism Prohibited

Any attempt to harm or destroy District 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. Intentional attempts to degrade or disrupt system performance will be viewed as violation of District policies and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes, but is not limited to, the uploading or creating of computer viruses, system break-in utilities, or system hacking programs.

Forgery Prohibited

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

Information Content/Third Party Supplied Information

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems outside the District's networks that may contain inaccurate and/or objectionable material. Any attempt to circumvent the filtering software is a violation of District policy.

A student bringing prohibited materials into the school's electronic environment will be subject to disciplinary action which could result in loss of credit for students.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. This could result in termination of employment for employees.

Network Etiquette

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

1. Use appropriate language on the RCISD system: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
2. Pretending to be someone else when sending or receiving messages through the RCISD system is prohibited.
3. Submitting, publishing or displaying through the RCISD system any defamatory, purposely inaccurate, racially offensive, abusive, discriminatory, bullying, obscene, profane, sexually oriented, harassing, threatening, damaging to another's reputation, or illegal materials or messages either public or private.
4. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Suspension/Revocation of System User Account

The District will reserve the right to suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulation regarding acceptable use.

Termination of an employee's account or of a student's access will be effective on the date the principal or RCISD Administrator provides notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Consequences of Improper Use

Improper or unethical use may result in disciplinary actions consistent with the existing **Student Code of Conduct** or **Employee Handbook**, and if appropriate, the Texas Penal Code, Computer Crime, Chapter 33, or other state and federal laws. This may also require financial restitution for costs associated with the system restoration, hardware, or software costs.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor-supplied hardware and software; therefore, 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 user's requirements nor that the data will be compatible with non-RCISD systems. Neither does the District warrant that the system will be uninterrupted or error-free, nor 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 necessarily the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks.

Nothing in this acceptable use policy creates any contractual right for the user.

Term

This policy is binding for the duration of the employee's employment or student's enrollment in RCISD. Students and employees will be required to review the District's Acceptable Use Policy on an annual basis and sign a receipt and acknowledgement form.