

Robstown ISD Acceptable Use Policy

User's Guidelines Purpose and Rights

All District guidelines and procedures for acceptable use of technology are intended to make the district's equipment, applications/programs and the system network more efficient, accessible and reliable for all "users."

The use of the District's computer equipment and the participation in any online communication services (i.e. Internet, e-mail, distance learning, Intranet and web pages) is a privilege and not a right. User must also follow all requirements and expectations of Student Conduct. User shall understand RISD will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate.

"User" is defined as Robstown ISD students, employees, volunteers, community members, and guests with access to a computer, Internet, and other technological equipment and software through the District.

Audits - Electronic auditing shall be implemented within all unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall be capable of recording:

- Access to the system, including successful and failed login attempts, and logouts;
- Inbound and outbound file transfers;
- Terminal connections to and from external systems;
- Sent and received e-mail messages;
- Web sites visited, including uniform resource locator (URL) of pages retrieved;
- Date, Time, and user associated with each event.

District Computer/Software Usage

Defining Computer/Software Usage Rights/Purposes:

The Computer/Equipment at Robstown Independent School District is to be used for instructional and administrative purposes. Instructional purposes include academic research, completing class assignments, communication, publishing, technology integration, technology proficiencies, software training and any activities that support the District's instructional objectives. The district has the right to monitor, audit, and review any files stored in district computers and any district electronic data devices as deemed appropriate to support identification, termination, and prosecution of unauthorized activity.

The following rights apply to all users:

1. District computers located in public areas (classrooms, labs, media centers) will be available for all users. A few computers may be restricted to certain user groups.
2. Some computers/equipment (i.e. software, digital cameras, laptops, etc.) will be available for use on a check out basis.

Acceptable Conduct

1. Users shall protect the security and privacy of RISD's systems and network.
2. Users shall treat computers with care. Information in proper computer care is provided by the Technology Department upon request.
3. Users who check out equipment/software shall be responsible and must make sure that equipment is operating properly prior to being checked out. It is also the responsibility of the user to return the equipment in the same condition it was checked out. (Normal wear and tear accepted).
4. The District has the right to monitor all computer usage.
5. Users shall obtain written permission before opening, moving, deleting, or duplicating the computer files of others.

Limitation of Uses

1. Users shall not hack or otherwise alter programs or files belonging to other users.
2. Users shall not take actions that are harmful to the district's equipment (vandalism).
3. Users shall not install software (i.e. games) not approved by the Technology Department IT Coordinator.
4. Users shall not use the computer/equipment in any way that may harass, defame or demean others with language,

image or threats.

5. Users shall not use computer/equipment for personal use such as for commercial purposes, financial gain, advertisement, and seeking/interacting with professional unions, political lobbying, supporting illegal activities.
6. Users shall not use/download any peer-to-peer (PTP) software such as Napster, Imesh, Morpheus, Kazza, etc.
7. Users shall not make any changes to the computer/equipment configurations (i.e. network settings, display settings including backgrounds and screen savers).
8. Users shall not use unauthorized administrative logins and passwords without the written approval from the Technology Department.
9. Users shall not write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan Horse, or similar name.
10. Users shall not use a diskette without initially running district approved virus scan software.
11. Users shall not assemble or disassemble computers/equipment without written permission from the Technology Department Administrator.
12. Users shall not move computer/equipment from designated areas without the written permission of the Technology Mentor or administrator. (An Inventory Transfer Form must be completed and turned in to campus designee before move is made.)
13. Users shall not waste district resources (paper, ink, disk space, diskettes, etc.).

Software Installation/Usage Policy

All software purchase or acquisitions must follow outlined district policy.

- All software must be approved by the technology department before purchase and checked for compatibility with District equipment.

- Technician or Technology Mentor must install all software with license attached to work order.

- Software must be purchased by grade level or department.

- Software may not be purchased solely for individual use unless approved by technology administrator.

1. District technology staff has the right to remove any unauthorized software on any District/Campus computers.

This includes but is not limited to:

- any peer-to-peer (PTP) software such as Napster, Imesh, Morpheus, Kazza, etc.

- screen savers or desktop themes

- software without license or documentation

- unauthorized downloaded software

- software that has not been approved or was not obtained through a purchase order

2. Restrict the use/listening of Internet radio stations or streaming of internet video to preserve District bandwidth.

3. Stop the use of games for staff and students with the exception of educational software that has been approved by the District.

Internet Usage

Defining Internet Usage Rights/Purpose

Robstown ISD is providing access to the Internet with the purpose to facilitate teaching and learning of the curriculum in accordance with Robstown ISD educational objectives. Therefore, Internet users must restrict their activities to endeavors in support of district educational and administrative objectives. The district has the right to monitor, audit, and review user's Internet access in district computers and any district electronic data devices as deemed appropriate to support identification, termination, and prosecution of unauthorized activity.

The following procedures will be applied at all campuses:

1. The Technology Mentor and/or Technology Department personnel will provide training in the proper and ethical use of the Internet and will provide all users with copies of the Electronic Communication and Data Management Guidelines.
2. The district shall monitor and/or review individual usage of the Internet to ensure its proper use. The district uses Lightspeed TTC (Total Traffic Control) to filter content and sites that are considered inappropriate.
3. The district has the right to generate a User Access Report detailing all violations. A report will be generated if: the user abuses the privilege of Internet access, is locked out by TTC, violates any of the guidelines, or is suspected of misusing the Internet.

Acceptable Conduct

1. Users shall use the Internet for educational and administrative purposes and as a tool to enhance teaching and learning in the classroom.
2. Users shall use Internet resources in accordance with copyright law. Copyright is implied in all cases whether or not explicit reference to copyright is mentioned.
3. Users shall use the Internet in accordance with civic and federal laws.
4. Users shall conserve district resources (paper in printer, disk space, bandwidth, etc.).

Limitation of Uses

1. Users shall not use the Internet for non-educational purposes.
2. System users shall not use or redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, district policy, and administrative regulations. Users will be held accountable for the use of copyright protected material obtained from third parties in the case where these parties are in violation of copyright law.
3. Users shall not use the Internet unless they have returned the appropriate agreement form signed and parents have agreed to allow use of the Internet.
4. Users shall not distribute personal information about themselves or others through the Internet.
5. Users shall not use the Internet in any capacity to gain unauthorized access to resources or information, or to maliciously attempt to harm or destroy district equipment or data, or the equipment or data of any of the agencies or other networks that are connected to the Internet.
6. Users shall not use District Internet access to conduct buying, selling, or promotion of commercial items.
7. Internet users shall not purposefully access or post materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's image, or illegal. These items include but are not limited to the following categories:
 - a) Adult -URLs with content intended for adults only. Examples include: Images or text that are provocative, suggestive, and erotic.
 - b) Sites which promote activities which are illegal for minors (such as drinking alcohol)
 - c) Other contents which many people may find repulsive or disgusting.
 - d) Crime -URLs which are intended to teach/instruct the reader in skills which are generally only useful for pursuing criminal activities, such as:
 - Building bombs or explosives
 - Hacking into computer systems
 - Lock picking
 - e) Drugs -URLs which promote the use of illegal controlled substances or instruct the reader how to grow/make/process these substances.
 - f) Entertainment - URLs, which allow the playing or downloading of games.
 - g) Gambling - URLs, which allow for on-line gambling or are dedicated to gambling information and instructions.
 - h) Intolerance - URLs, which advocate intolerance or hatred of a person or group of people.
 - i) Violence- URLs, which show or advocate violence. Examples include: Images containing graphic violence (blood/murder), promotion of violence or terrorist acts against others.
8. Users shall not gain unauthorized access to resources or information.
9. Users shall not waste system resources while using the Internet. Examples of resource waste violations are:
 - a) Printing items that not educational
 - b) Downloading large files, such as games, multimedia programs, music and videos

Chat Rooms and Newsgroups Usage

Defining Chat and Newsgroup Usage Rights/Purpose

Users shall not participate in newsgroups or chat rooms. With approval from the Technology Department, chat rooms and newsgroups can be made available for educational use and only for a limited time. Teachers may assign projects requiring educational chats with other students/professionals by completing a request form and notifying their Technology Mentor in advance so arrangements may be made.

1. The district has the right to block chats.
2. Even if user has district approval to use a chat line/room, the district has the right to lock out any user that uses chats excessively, in an inappropriate manner, and/or in violation of the guidelines outlined below.
3. The district has the right to decide which chat lines are educational.

Acceptable Conduct

1. With prior, written permission, users shall use educational chat rooms, network chat, or newsgroup accessed on the Internet for educational purposes.

Limitation of Uses

1. Users are prohibited from participating in any chat room, without proper approval.

Electronic Mail Usage

Defining Certain Rights/ Purpose

The purpose of the school district's E-mail is to facilitate communications in support of research and education. Access to the district's E-mail system is a privilege, not a right. Users of the district E-mail system are required to comply with all District rules, regulations, and policies governing appropriate use of the system. Users should be mindful that use of school related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.

The following procedures will be applied at all campuses:

1. The Technology Department will create e-mail accounts. Therefore, campuses must provide proper documentation to the Technology Department for the creation of e-mail accounts.
2. Users shall not share their login or password with anyone.
3. E-mail transmissions sent and received by students and employees are not private and may be monitored if suspicion concerning inappropriate use exists.
4. District has the right to monitor and review sent or received mail to ensure proper and ethical usage of E-mail.
5. The district has the right to access a User Content Report detailing any violations through E-mail.
6. District has the right to deny the privilege of using E-mail to any user who is in violation of any guideline outline below.
7. Supervisors have the right to request, from the Technology Department, copies of E-mail sent or received by staff if suspicion concerning inappropriate use exists.

Acceptable Conduct

1. Users shall use E-mail for educational purposes and must be consistent with the educational mission of the Robstown Independent School District.
2. Users shall attend the district's training in order to obtain an authorized E-mail account.
3. Users shall purge electronic mail on a regular basis to ensure proper use of system.
4. Users shall report illegal or unauthorized use of the E-mail or online systems to the Technology Mentor and/or Technology Department.

Limitation of Uses

1. Users shall not use the E-mail system for any illegal activity, including but not limited to violation of copyright laws (plagiarism, forgery).
2. Users shall not transmit personal information about students including, but not limited to student names, phone numbers and addresses outside of the district's network without written permission from the student (i.e. 18+) or his/her parents.
3. Users shall not use E-mail to sell or to solicit products or services. Users shall not use Email for private or commercial offerings of products or services.
4. Users shall not use and/or respond to E-mail in any way that would be considered:
 - a) Damaging to another's reputation
 - b) Abusive
 - c) Obscene
 - d) Sexually oriented

- e) Offensive
 - f) Threatening
 - g) Harassing
 - h) Illegal
 - i) Contrary to school policy
5. Users shall not attempt to read, delete, copy, or modify the E-mail of any other user.
 6. Users should not deliberately interfere with the ability of other users to send/receive E-mail.
 7. Users shall not use the E-mail system in a fashion that is inconsistent with directions given during training.
 8. Users shall not use the E-mail system to distribute material or information on behalf of or with regard to professional unions, collective bargaining, private businesses or associations, or political campaigns or organizations without the express written consent of the Superintendent or designee.
 9. Users shall not access private E-mail accounts such as HOTMAIL, YAHOO MAIL, etc. when using the district's Internet system.
 10. User shall not use E-mail for the purpose of sending unnecessary or junk mail.
 11. Users shall not respond to unsolicited E-mail messages from any source without the permission of the technology department.
 12. User shall not pretend to be someone else when sending/receiving messages.
 13. Users shall not use E-mail for any purposes that may present a tangible cost to the school or interfere with the operations of the computer network or with the performance of the student or employees.

Developing and Publishing of Web Pages

Defining Web Pages Usage Rights/Purposes

Web sites should be primarily academic in nature. They may also serve to support our educational programs by informing our community about events and activities and reflect the unique personality of each school. Users should be mindful that publishing a web page on RISD's web server might cause some recipients or other visitors of that web site to assume they represent the District or school, whether or not that was the user's intention.

1. The following criteria must be considered when creating and/or posting material to a web page:
 - a) Requirement of the District's web administrator to upload campus/district's web pages.
 - b) Maintenance includes (but is not limited to) timely updating.
2. Roles and responsibilities of the developers in the web creating/posting process:
 - a) Web Site Administrator: Responsible for all web sites residing on RISD servers. Has the authority to add, edit, and delete any web link, image, page, folder, and site. Administrator has FINAL say on any and all content existing on district web servers.
 - b) District Web Master: Responsible for all web pages placed on the web server for Robstown ISD. The district web master may shut down pages on any web site that uses excessive system resources or network bandwidth.
 - c) Campus Web Master: Designated by the Technology Department or campus administrator to act as managing editor for the campus web site. Permission of originator is needed to publish information, graphics and/or photographs on the Internet. Web master will be responsible to gather all Copyright Permission Letters from the Web team and turn them in to the Web Site Administrator before publishing.
 - d) Web Team: Team of staff and/or students under the direction of the web master and/or advisor, which includes co-writers, designers and web editors. The team is responsible for establishing, maintaining, and accommodating the newly acquired pages for the school's web site. Periodic checks of external links and the ongoing upkeep of the web site are required.
3. Permission form must be signed by student (i.e., 18 yrs +) and/or parent prior to the publishing of the student's work. These forms must be turned in to the web site administrator.
4. Web pages created by employees belong to the district even if the employee is no longer in the district.

The following rights apply to all users:

1. The district has the right to deny publishing a school's or a department's web page that does not follow the approved districts web page template.
2. The district's web master or district web administrator has the right to delete any web page that uses excessive system resources or network bandwidth or that is in violation of any of the guidelines outlined below.

Acceptable Conduct

1. Users shall publish school-related web pages. Web pages' content and the intent shall be in accordance with the Robstown Independent School District's Internet policies and guidelines.
2. Users of web pages shall be in compliance with federal copyright laws.
3. Users shall obtain permission from originator in order to publish information, graphics or photographs on any school related web page. All graphics, photos, and art must include site references.
4. Users (students) shall obtain and file, with the web administrator, a signed permission form prior to publishing student's work in the Internet.
5. Users' web pages shall be appropriate in relation to the objectives of the class/campus/district.
6. Users, who publish a school-related web page on the Internet, shall use only the campus/district's web servers to publishing their WebPages.

Limitation of Uses

1. Users shall not use excessive resources on web pages.
2. Users shall not create campus and departments' web pages without using the district's approved template. Teachers and students individual web pages do not need to follow the approved district's web page.
3. Users shall not publish web pages for commercial or private advertising, commercial offerings of products or services for sale, or solicit products or services or to raise funds for non-district related activities or organizations.
4. Users of web pages shall not use the network to disseminate material or information on the behalf of or with regard to professional unions, collective bargaining, private businesses or associations, or political campaign organizations without the express written consent of the Superintendent.
5. Users who create school-related web pages shall not publish their work outside of the districts web server. (i.e. local provider, geocities.com, etc)
6. Users shall not identify students on school's web pages. Users shall follow these guidelines:
 - a) When appropriate, first initials and last names or first name along with initial of last name shall be used. Complete first and last name can be listed with parent permission.
 - b) Student work shall not reveal family or personal details that may be construed as invasion of privacy for student or family members.
 - c) Student pictures shall not be published unless written parental permission or student (i.e., 18yrs +) permission is obtained. Group pictures are recommended, with references to teacher's class rather than individual names.

Distance Learning Videoconference Usage

Defining Certain Rights/Purposes

Distance learning is two-way communication between a teacher and student separated by distance, using technology for facilitating and supporting the curriculum. Videoconferencing is one form of distance learning where two or more distant groups communicate "face-to-face", in real time, by using audio and video equipment. It brings people in one location together with those in another-whether it be from a university to a medical institution or from a junior high to a library-allowing them to share their knowledge, experiences, and backgrounds.

Note: 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.

Only a district employee may request to use the distance learning system and in doing so will be ultimately responsible for use of the system.

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 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 interrupted or error free, or that defects will be corrected.

Acceptable Conduct

1. Users shall be observant that the use of school-related videoconference system might cause some recipients to assume they represent the District or school, whether or not that was the user's intention.
2. Users (students) shall follow all rules as specified by the teacher.

Limitation of Uses

1. Users shall not use the system in any way that violates copyright laws. Educational institutions and organizations are not exempt from copyright laws. These laws provide protection for literary works; musical works, including accompanying words; dramatic works, including accompanying music. In addition, pantomimes and choreographic works; pictorial, graphic and sculptural work; motion pictures and other audiovisual works; and sound recordings are also protected. In the distance learning setting, what may have been considered "fair use" in the traditional classroom may be transformed into a public performance. Therefore, educators must have permission from the owner of the copyright to use copyrighted materials during the "performance."
2. Users in grades Pre-Kinder through twelfth shall not participate in the District's videoconferencing system with their teachers or facilitator without consent from their parents.
3. Users shall not bring prohibited materials into the school's electronic environment.
4. Users shall not say, send, post messages, or use hand gestures that are abusive, obscene, sexually oriented, threatening, harassing, or damaging to another's reputation.
5. Users shall not maliciously attempt to harm or destroy district's Distance Learning Videoconference system, or any of the agencies or other networks that are connected to the District's system.
6. Users shall not use the system for illegal purposes, in support of illegal activities, or for any other activity prohibited by District's policy or guidelines.
7. Any original work created by users shall not be included in a videoconference session under the District's control unless the District has received written consent from the student and the student's parent.
8. Users shall not interfere with the teaching or learning in the classroom.

Disciplinary Action

Electronic Communication and Data Management System (Technology)

Students must follow all District's Electronic Communication and Data Management Guidelines when using district computers or when participating in a school-related activity.

Violations of the Student Code of Conduct with the use of district's computers and networks will result in disciplinary action as stated in the Student Code of Conduct Handbook.

The severity of the violation committed using technology will result in the severity of disciplinary action.

Deliberate attempts to degrade or disrupt system performance are violations of the District's Electronic Communication and Data Management Guidelines and may constitute criminal activity under applicable state and federal laws. The district will cooperate fully with local, state, and federal officials in an investigation concerning or relating to the misuse of any electronic communication and data management system.

The user causing the system's damage must reimburse any costs that the district incurs due to the misuse or abuse of the system.

Violation/Offense (Level I)

Any violations of the limitations of usage within these guidelines will be considered a Level 1 violation; unless the violation is classified as a Level II violation.

Recommended Consequences for Level I Violation/Offense

Student Offenders

1st time offense ? warning by teacher

2nd time offense ? loss of privilege to use computer until conference held with parent and administrator or designee

3rd time offense ? loss of privilege to use computer for time determined by principal or designee

District Staff Offenders

1st time offense ? warning by administrator

2nd time offense ? loss of privilege to use computer until conference held with administrator or designee

3rd time offense ? loss of privilege to use computer for time determined by principal or designee

Violation/Offense (Level II)

The following violations are immediately considered level 2 offenses.

- Take actions that are harmful to the district's equipment (vandalism).
- Use the computer/equipment in any way that may harass, defame or demean others with language, image or threats.
- Attempt to use or discover any password used for administrative software and hardware to gain illegal entry.
- Write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan Horse, or similar name.
- Assemble or disassemble computers/equipment without written authorization from the Information or Instructional Technology Director.
- Malicious attempts to harm or destroy district equipment or data, or the equipment or data of any of the agencies or other networks that are connected to the Internet.
- Purposely access or post materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's image, or illegal. These items include but are not limited to content filtering software categories under the Internet Usage section (Limitations of usage, #7).
- Say, send, post messages, or use hand gestures that are abusive, obscene, sexually oriented, threatening, harassing, or damaging to another's reputation which using the video conferencing equipment.
- Hack or alter programs or files belonging to other users. For example, erasing, renaming, or making unusable anyone else's files, programs, email or disks.

Recommended Consequences for Level II Violation/Offense

Student Offenders

1st time offense - loss of privilege to use computer until conference held with administrator or designee. Parents will be notified of the offense. Reimbursement must be made for any costs that the district incurs due to the misuse or abuse of the system. Authorities may be notified at administrators' discretion. All possible legal actions will be taken against offenders.

2nd time offense - loss of privilege to use computer for time determined by principal or designee and any consequence determined by principal as appropriate for the violation. Parents will be notified of the offense. Reimbursement must be made for any costs that the district incurs due to the misuse or abuse of the system. Authorities may be notified at administrators' discretion. All possible legal actions will be taken against offenders.

District Staff Offenders

1st time offense - loss of privilege to use computer until conference held with administrator or designee. Reimbursement must be made for any costs that the district incurs due to the misuse or abuse of the system. Authorities may be notified at administrators' discretion. All possible legal actions will be taken against offenders.

2nd time offense - loss of privilege to use computer for time determined by principal or designee and any consequence determined by principal as appropriate for the violation. Reimbursement must be made for any costs that the district incurs due to the misuse or abuse of the system. Authorities may be notified at administrators' discretion. All possible legal actions will be taken against offenders.

Disclaimer of Liability

The District is not liable for inappropriate use of electronic communication resources, violations of copyright restrictions or other laws, mistakes or negligence, or costs incurred by users. The District is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.