ROCKDALE COUNTY PUBLIC SCHOOLS
ACCEPTABLE USE - REGULATION IFBG-R

I. Introduction

Each employee, parent, and student of Rockdale County Public School’s (RCPS) information system is expected to be familiar with and follow the expectations and requirements of the Acceptable Use Policy (AUP). The purpose of the AUP is to ensure that individuals are aware of their responsibilities regarding the Internet and related technology and equipment. This AUP also helps ensure the safety and privacy of current and former employees and students.

A. Legal Requirements

RCPS is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

- The Family Educational Rights and Privacy Act (FERPA)
- Children's Internet Protection Act (CIPA)
- Individuals with Disabilities Education Act (IDEA)
- Section 504 of Rehabilitation Act of 1973 (Section 504)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPPA)

Users of RCPS's network are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies through the use of RCPS networks may result in discipline (including termination or expulsion) or litigation against the offender(s) by the proper authority. RCPS will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

B. Acceptable Use

RCPS provides computer, network, e-mail, and Internet access to individuals as part of the learning environment. The use of these resources is a privilege and not a right and may be revoked at any time without notice. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use by every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline (including termination or expulsion) or litigation in accordance with board policy and state and federal law.

II. Employee Acceptable Use

This section is dedicated to provide RCPS employees with guidance of acceptable use of the District's information technology resources, including but not limited to:

- The internet, intranet, e-mail, and district portal.
- District assigned computing devices such as personal electronic devices, laptops and desktops, and
- The District's network and supporting systems and data transmitted by and stored on the RCPS systems.

A. Annual Responsibilities and Information Security Awareness

Staff members will review the Acceptable Use Policy presented on the RCPS Portal website annually.
B. Prohibited Use of RCPS Resources

The following uses of RCPS computer resources by staff members are prohibited at all times:

- Personal use is prohibited.
- Infringing upon the intellectual property rights of others or violating copyright laws.
- Advancing personal profit.
- Furthering political causes in violation of board policy or the state Code of Ethic for Educators.
- Uploading or transferring out of the District's direct control any software licensed to the District or data owned by the District without explicit written authorization. Failure to observe copyright or license agreements can result in disciplinary action from RCPS or legal action by the copyright owner.
- Unauthorized use of resources (including but not limited to servers, networks, computers and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms.
- Downloading software unless it is required to complete their job responsibilities and approved and implemented by the District’s technology department.
- Bypassing or attempting to bypass any of the District's security or content filtering safeguards.
- Accessing or attempting to access resources for which an employee does not have explicit authorization by means of assigned user accounts, valid passwords, file permissions, or other legitimate access and authentication methods.
- Granting another individual access to any District accounts that have been authorized to you or using another individual's District authorized accounts, user-id and/or password. Specific exceptions are allowed for the District’s technology department personnel for authorized system operations and maintenance.
- Allowing another person to use a District system under his or her login.
- Adding, modifying, repairing, removing, reconfiguring, defacing, or tampering with any RCPS device.
- Allowing non-district persons permission to use District assigned information systems on District equipment taken off-site.
- Sharing the password of their unique RCPS user ID or using this password to access other 3rd party web sites or applications.
- The use of any "hacking tools" that can be used for "computer hacking", may not be possessed on school property, on any District premise, or run or loaded on any District system.
- Violating any state or federal law or regulation, board policy or administrative rule.

C. Supervision and Monitoring

It shall be the responsibility of all members of RCPS staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and CIPA.

In addition, the faculty and staff of RCPS will provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the District’s technology department or designated representatives.
D. Sensitive Information

RCPS employees who have or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and other applicable laws and regulations, as they relate to the release of student information.

- Employees may not disclose sensitive or personally identifiable information regarding students to individuals and/or parties not authorized to receive it. Authorization to disclose information of a student to individuals and/or parties must strictly adhere to regulations set forth in the FERPA.
- Information contained in these records must be securely handled and stored according to RCPS directives, rules, and policies, and if necessary destroyed in accordance with state information retention standards and archival policy.

Each District e-mail user is responsible for the content of all text, audio, video, or images that he or she places or sends over the Internet or District email systems.

- An employee must preserve all emails and other relevant records related to an incident that is subject to litigation once that employee is made aware of the legal action.
- RCPS does not grant any ownership, privacy, or an expectation of privacy in the contents of any message, including e-mail, or other Internet activities involving RCPS resources or equipment.

E. Consequences

Employees who violate this administrative rule may be subject to discipline, including termination. All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to an employee’s supervisor and directly to the District’s Technology Help Desk. Suspected criminal activity must be immediately reported to law enforcement.

III. Student Acceptable Use

Rockdale County Public Schools strongly believes in the educational value of electronic services and recognizes the potential to support curriculum and student learning by facilitating resource sharing, innovation, and communication.

Access to the Internet allows students to explore thousands of libraries, databases, museums, and other repositories of information. All Internet access from Rockdale County Schools shall be through the Rockdale County network system except as may be required by the State Department of Education for specified administrative use.

Families should be aware that some material accessible via the Internet may contain items that are inappropriate, inaccurate, or potentially offensive. While the purposes of the school are to use electronic resources for constructive educational goals, students may find ways to access other materials. The District believes that the benefits to students from electronic services in the form of information resources and opportunities for collaboration exceed the disadvantages. But, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Therefore, the District supports and respects each family's right to deny electronic services to their child by simply not signing the Acceptable Use Agreement.
Authorized student use of information resources must be consistent with the educational purposes for which these resources have been provided. The use of RCPS electronic services is to assist students in completing educational activities and should be used in a manner that enhances educational experiences and complies with RCPS policies. All student users must adhere to the provisions of this Acceptable Use Policy as a condition for continued use of the RCPS network. This policy must be followed anytime there is a connection to the District's wired or wireless network via any electronic device. RCPS reserves the right to monitor any user’s online activities. Users should have no expectation of privacy regarding their use of RCPS property, including devices, the network, Internet access, documents, files, chat rooms, learning management system, cloud storage, and e-mail.

A. Internet Safety

In compliance with the Children’s Internet Protection Act ("CIPA") [Pub. L. No. 106-554 and 47 USC 254(h)], Rockdale County Public Schools is required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate material on the Internet; (b) the safety and security of minors when using cloud storage, e-mail, learning management system, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called “hacking,” and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors’ access to materials harmful to them. Furthermore, each campus educates students on cyberbullying, appropriate online behavior, social networking, and other aspects of digital citizenship as required by CIPA.

- RCPS has implemented filtering and/or blocking software to restrict access to Internet sites containing pornography, obscene depictions, or other materials harmful to minors under 18 years of age, to the extent practicable, while using its network. However, no software is completely fail-safe, and there is still a risk a user may be exposed to a site or message containing such materials.
- The student’s parent or guardian is responsible for supervising and monitoring all computer usage that occurs outside the RCPS network.
- Students will not disclose personal information, including name, home address, telephone number, photos, and the like on the Internet or through software installed on RCPS electronic devices. Students are advised to never access, keep, or send anything that they would not want the general public to see.
- Students will not meet in person with anyone they have met only online via the Internet.
- The user is personally responsible for his or her actions in accessing and utilizing the school’s computer resources.
- Students must abide by all laws, regulations, the Student Code of Conduct, Acceptable Use Policy, and other related RCPS security policies.
- Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized for bona fide research or other lawful purposes.

B. Acceptable Actions

RCPS students may use the network and electronic services provided by RCPS to pursue educational activities. Students will learn how Internet resources can provide valuable educational information. Students will be expected to follow accepted rules of digital citizenship. These rules include, but are not limited to, the following:

- Be courteous and respectful. Do not send or display offensive messages or pictures.
- Use appropriate language in any type of communication. No profane, abusive, or impolite language will be used to communicate nor should materials be accessed that are not in line with the rules of school behavior.
- Keep personal information such as logins, passwords, addresses, and phone numbers confidential.
- Use electronic services for educational purposes only.
C. Unacceptable Actions

Improper use of electronic services provided by RCPS is prohibited. Students should be prepared to be held accountable for their actions and for the loss of privileges if this Acceptable Use Policy is violated. In addition to the paragraph below labeled “Penalties for Improper Use,” the RCPS Student Code of Conduct addresses the consequences for violations. Actions that constitute unacceptable use include, but are not limited to the following:

- Do not use a device to harm other people or their work.
- Do not damage or deface the device or the network in any way.
- Do not interfere with the operation of the network by installing software, shareware, or freeware, including the alteration of any controls designed to provide Internet safety or alteration of RCPS’s default computer settings.
- Do not violate copyright laws or participate in any criminal activities.
- Do not view, send, or display offensive messages, pictures, or other inappropriate content.
- Do not share your password with another person or offer access to any person via your account.
- Do not reveal your personal address or phone numbers or those of other students, including the completion of profile data.
- Do not waste limited resources such as disk space or printing capacity.
- Do not distribute advertisements, solicitations, commercial ventures, or political lobbying.
- Do not trespass in another's folders, work, or files.
- Do not pursue internal or external “hacking,” use anonymous e-mail sites or proxies, access illegal file sharing networks, spread viruses, intentionally transmit spam, or attempt to access inappropriate material.
- Do not take digital pictures or video without teacher or administrator permission and for anything other than academic use.

IV. Other Terms of Use

A. Penalties for Improper Use

The use of the network is a privilege, not a right, and may be revoked if abused. Misuse, damage, or vandalism of RCPS technology resources may also lead to disciplinary and/or legal action, including suspension, expulsion, or criminal prosecution by governmental authorities.

B. Expectation of Privacy

Individuals should not have an expectation of privacy in the use of the District's email, systems, or equipment. The District may, for a legitimate reason, perform the following:

- Obtain emails sent or received on District email.
- Monitor an individual's use on the District's systems.
- Confiscate and/or search District-owned software or equipment.

C. Disclaimer
RCPS makes no guarantee about the quality of services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from the use of its network. Any charge accrued to the user of RCPS’s network are borne by the user. Statements by the user on the Internet are from the author’s individual point of view and do not represent the views of RCPS, its employees, or members of the Board of Education.

Employee, Student and parental/guardian signatures on the Acceptable Use Agreement represent consent to conform to the Acceptable Use Policy.