Technology Acceptable Use Policy

Introduction

All use of Russell County School District network resources, including the Internet, shall be consistent with the District's goal of promoting excellence by facilitating resource sharing, innovation and communication. Russell County Schools relies on its computer network to enhance education outcomes. To ensure that RCSD'S computer resources are used properly by its employees, students, independent contractors, agents, vendors, and other computer users, the Russell County Board of Education has drafted and approved the following Responsible Use Policy.

The rules and obligations described in this policy apply to all users of RCSD'S computer network or computer resources, wherever they may be located in RCSD'S policies. Specific policies against discrimination and harassment (sexual or otherwise) apply fully to RCSD'S computer resources, and any violation of these policies serves as grounds for discipline up to and including termination. Students who violate these policies are subject to disciplinary action consistent with Board policy and the Student Handbook. Vendors, consultants, and all other third party guest users must adhere to these policies and are subject to losing their right to access RCSD'S computer resources for violations of these policies.

By complying with the provisions in this Responsible Use Policy, users consent to monitoring as a condition of access under the Electronic Communications Privacy Act (1986). All users should be aware that RCSD'S computer resource uses including all its components are subject to monitoring in order to comply with the Alabama Supercomputer Authority and Family Educational Rights and Privacy Act (FERPA), as well as the Children's Internet Protection Act (CIPA). Employees, students, and other users should not have any expectation of privacy in anything they create, store, send or receive using the RCSD'S computer resources. The main goal of this aspect of the Responsible Use Policy is to ensure our children's safety and protection while using technology for educational purposes.

All technology resource use will be governed by the requirement that it must add to the standards-based educational experience and growth of the user and not disrupt the educational process in anyway.

Policy Statements

The Children's Internet Protection Act (CIPA) is a federal law that addresses concerns about access in schools and libraries to the Internet and other information. Under CIPA, schools and libraries are required to certify that they have certain Internet safety measures in place. These include measures to block or filter pictures that: (a) are obscene, (b) contain child pornography, or (c) when computers with Internet access are used by minors, are harmful to minors. Schools subject to CIPA are required to adopt a policy to monitor online activities of minors i.e. (a) access by minors to inappropriate matter on the Internet and the Web; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications, including but not limited to social networking sites; (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) restricting minors' access to materials harmful to them.

Schools will annually provide for the educating of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

Technology Acceptable Use

Access to the District's network resources, including the Internet, must be for the purpose of education or research, and be consistent with the educational objectives of the district. Transmission of any material in violation of United States or state statute or regulation is strictly prohibited. This includes but is not limited to copyright or trade secret material, threatening or obscene material, and criminal activity. The use of the network resources for commercial activities, product solicitations, or political lobbying is also prohibited. Inappropriate use will be reported to the responsible authorities.

No warranties - The District makes no warranties of any kind, whether expresses or implied, for the service it is providing. The District will not be responsible for any damages. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by negligence or user errors or omissions. Use of any information obtained via the Internet is at the authorized user's own risk. The District specifically denies and responsibility for the accuracy or quality of information obtained through its services.

Technology Unacceptable Use

The taking, disseminating, transferring, or sharing of obscene, pornographic, lewd, or otherwise illegal image or photographs, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, etc.) may constitute a CRIME under state and/or federal law. Any person taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images or photographs will be reported to law enforcement and/or other appropriate state or federal agencies, which may result in arrest, criminal prosecution, and LIFETIME inclusion on sexual offender registries.

Some examples of unacceptable uses are:

- Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State Law.
- Unauthorized installation of software, regardless of whether it is copyrighted or de-viruses including the unauthorized installation of software.
- Downloading copyrighted material for other than personal use.
- Using the network for private financial or commercial gain.
- Wastefully using resources, such as file space.
- Gaining unauthorized access to resources or entities.
- Invading the privacy of individuals.
- Using another user's account or password.
- Posting material authorized or created by another without his/her consent.
- Posting anonymous messages.
- Using the network for commercial or private advertising.
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material.
- Using the network while access privileges are suspended or revoked.

Any user who violates this policy may have computer/Internet privileges revoked at any time and without prior notice. Employee violations of this policy may also result in administrative leave, suspension, and possible termination. Student users are also subject to discipline according to the Russell County Student Code of Conduct. Any illegal use will also result in civil and/or criminal liability.

Social Media

Russell County Schools recognizes the value of social media, both for personal and professional use. However, there are some guidelines that should be addressed when educators use social media. The guidelines and reminders below have been developed to better protect (and inform) RCSD employees from charges of inappropriate use. Teachers should not “friend” students on personal social media. Teachers should also be judicious about "friending" students' parents on social media. Unacceptable Social Media Use Includes:

- Updating social media or posting non-instructional content during school hours.
- Posting pictures with students in them without permission of parents or guardians.
- Using social media as the sole means of classroom communication.
- Posting disruptive content which harms the goodwill and reputation of the students, teachers, school, and system.

Communication between teachers, parents, and students should be of an educational/extra-curricular nature and support the vision, mission, and beliefs of RCSD. Other types of personal communication between teachers and students must be avoided.

Definitions

“computer resources” as used here in refers to RCSD’S entire computer, electronic and communications network.

“Users” include employees, substitutes, students, and guests, using technology, including, but not limited to computers, networks, Internet, email, chat rooms, and other forms of technology services and products.

“Network” is wired and wireless technology networks, including school and district networks, cellular networks, commercial, community or home-based wireless networks accessible to students.

“Equipment” includes cellular phones, smart phones, PDAs, MP3 players, iPod-type devices, and portable computers such as laptops, iPads, Nooks, Chromebooks, desktops, tablets and netbooks, as well as portable storage devices.