RCS TECHNOLOGY USE POLICY - Policy 4055

Policy

Rochester Catholic Schools (RCS) continues to integrate computer and network technology into its educational and professional environments. As part of that effort, this policy and supporting guidelines are to provide direction and safety to our technology users and students, as well as to protect our technology assets.

General Statement of Policy:

- All computer and technology equipment will be used in a manner that is consistent with the mission and goals of RCS.
- The use of computer, technology and network equipment is integral to a quality education and working environment.
- Inappropriate use will result in disciplinary or law enforcement action.
- RCS' employees, contractors, students and volunteers shall abide by the procedures established to support this policy.

Procedure:

I. Types of Technology:

Desktop computers, laptop computers, Chromebooks, iPads, tablet computers, netbook computers, LAN telephones, pagers, cell phones, smart phones, audio or video equipment, projectors, PA systems, cameras, and any network attached and wireless equipment, services and accounts (Windows accounts, G Suite for Education accounts) and all apps and software.

II. Scope:

This policy covers all computers and technology equipment, services and accounts (including RCS Windows accounts and G Suite for Education accounts) owned or managed by RCS, both on and off campus. It also refers to personal computer equipment and other personal technology used on campus, at RCS sponsored events or on field trips where applicable rules apply.

III. Technology Use Agreement:

All RCS students, grades 4 through 12 and all employees, contractors and volunteers using RCS technology must read the Rochester Catholic Schools Technology Use Agreement at the beginning of each school year and before using RSC technology or personal technology in RCS school buildings, at RCS sponsored events or on field trips. All Grade 4 students, all newly enrolling Grade 5-12 students and all newly hired or assigned employees, contractors and volunteers must also submit a signed copy of the signature page at the end of this document to the RCS Department of Technology before using RCS Technology. The purpose of this agreement is to ensure that RCS students, employees, contractors and volunteers using RCS technology have read, understood, and agree to the RCS Technology Use Policy.

A. General Rules:

1) All use of technology must reflect the Christian ethics, values and teachings consistent with the mission and goals of RCS and the Roman Catholic Church. All use must be appropriate for enabling and advancing student learning and/or for the efficient operation of RCS. Inappropriate use will not be tolerated and may result in disciplinary action. Illegal activity will result in law enforcement action.
2) Only authorized individuals may use RCS owned technology. Visitors, employee spouses and their non-enrolled children, as well as other non-enrolled or non-employed individuals, may not use, move, or modify RCS technology without the expressed consent and guidance of the respective building administrator or the Director of Technology.
3) No RCS owned non-mobile technology may be removed from RCS premises without the express consent of the respective building administrator or the Director of Technology. Use of RCS owned mobile technology (iPads, Chromebooks, laptops, etc.) is governed by explicit, signed loan agreements, and users must adhere to the loan agreement guidelines.
4) No RCS Desktop systems are to be moved to a new location without the direct involvement of the RCS Department of Technology. No computer ID labels are to be altered, removed or tampered with.
5) Technology parts, components, peripherals, configurations, system settings and applications may not be altered, added to, disconnected, or removed without permission or assistance from the Department of Technology for RCS owned technology.
6) Technology problems should be reported in a timely manner to the Department of Technology through the appropriate support channel: http://support.rcsmn.org/
7) RCS owned and licensed software may be used only on RCS owned computers, or in specific accordance with the software licensing agreement.

8) RCS students, employees, contractors, or volunteers must not encrypt files or data on RCS systems or networks, unless explicitly authorized by the appropriate building administrator or the Director of Technology.
9) Information on the Internet that is considered obscene, offensive, and questionable in nature shall not be accessed anywhere using RCS owned technology, or within RCS premises.
10) RCS has hardware and software that prevents access to inappropriate Internet information through its staff and student networks and the guest wireless network.
    a. If a valid web site cannot be accessed, a report may be filed through the appropriate technical support channels.
    b. If an inappropriate website has been accessed freely, the website's complete address should be reported to the building administrator and the Director of Technology for further action.
    c. Since RCS cannot filter content delivered via public networks (for example, wireless networks provided by cell phone companies) RCS students may only use personal technology on RCS premises, during RCS sponsored events or on field trips when under the appropriate supervision of RCS staff.
    d. RCS students, employees, contractors, volunteers and visitors must not make use of any software or hardware that bypasses RCS network security, firewall protection, or web content filtering. This includes but is not limited to the use of web proxy or VPN software or tools.
    e. RCS students, employees, contractors, volunteers and visitors must not make use of any mobile wireless hotspots while on RCS premises. RCS provides a public and a guest wireless network that should meet the needs of all.
11) Network users shall not log onto an RCS workstation, web or email account using someone else's user name and/or password. Network users shall not allow another person to use their network user, web or email account for any reason. Network users must contact the Department of Technology immediately if they suspect any of their account(s) have been misused or their password(s) compromised.
12) Network users will be required to change their password periodically. Your network administrator determines the frequency of change, minimum password length and complexity.
13) Network users must not share their passwords with anyone, nor allow their passwords to be exposed to or seen by any other person. (Please note: special password management rules will apply to young students in grade 3 and lower.)
14) Network users must log off or lock their workstations or mobile devices before leaving them unattended.
15) Personal information about yourself or others, such as addresses and phone numbers, should never be given to anyone online.
16) Inappropriate use of technology should be reported immediately. Staff must notify their building administrator or the Director of Technology. Students must notify their teacher or another responsible adult.

17) Exceptions: The Director of Schools may grant limited exceptions to the provisions in this document in cooperation with the Director of Technology in order to meet the immediate needs of the educational environment or as new technology or new uses emerge. Any exception to this policy will require advance approval in writing from the Director of Technology and the Director of Schools.

B. Rules Specific to Rochester Catholic School Students:

1) RCS students are allowed to use RCS owned technology in a manner that is consistent with the rules outlined in this document and their parent/student handbook. RCS Students are expected to use RCS owned Technology for schoolwork or homework only. Priority of access to technology will be given to students doing required academic work.
2) RCS students are allowed to use RCS owned non-mobile technology only under the direct supervision of an RCS employee. RCS owned student mobile devices must be used in accordance with the device loan agreement.
3) Students will be provided with computer access, secure student computer accounts, an email account and storage space for school related work. Each student will be held responsible for all activity that is related to his/her account.
4) School staff, administrators and parents may be given access to student computers and email accounts for monitoring purposes. Students should have no expectation of privacy on their computer or email accounts. Students must comply with requests from their parent or an appropriate RCS staff member to inspect RCS owned devices or accounts; any attempts to hide or remove information from an inspection may result in disciplinary action.
5) No students may access information, servers or networks that are not public and to which they have no explicit permission to access.
6) No students may access RCS computers, systems or networks that are designated for the use of RCS staff only.
7) Prohibited uses of email, social networking sites, picture phones, YouTube, blog sites, etc.: Postings on the internet, even if the access to such postings is restricted to a predetermined “group list,” are, in fact, considered “public.” Therefore, a good deal of thought needs to be put forth in messages or postings. A prohibited use may result in discipline, including but not limited to requests to remove the posting, suspension, dismissal and referral to law enforcement authorities. The following are prohibited uses, on or off campus, at any time:
    a. Messages, content or postings that are demeaning, inflammatory, degrading, vulgar, or slanderous pertaining to any of the Rochester Catholic Schools or any of its employees, contractors, volunteers or students.
    b. Capturing, storing or transmitting pictures or video recordings of other RCS staff or students except:
        i. as part of a specific academic assignment or project under the direct supervision of an RCS teacher or advisor;
        ii. or with the prior written permission from the appropriate Rochester Catholic School administrator.
    c. Engaging in unlawful or criminal activity or gang-related activity.

d. Harassing, bullying, threatening or demeaning any person.
e. Inappropriate sexual or other offensive content.

8) Students agree not to meet with someone they have met online without their parent's approval and participation.
9) Students will tell their teacher or other school employee about any message they receive that is inappropriate or makes them feel uncomfortable.
10) Students will be held accountable for all transmissions originating from their personally owned email or social media accounts.
11) RCS issued student email accounts:
    a. An RCS issued student email account is exclusively for the intent of exchanging information consistent with the academic purposes and ethical policies of Rochester Catholic Schools.
    b. Student email accounts for grades 2-5 are limited to transmission within the RCS email domains only. No external email transmission is allowed. Any attempt to circumvent this limitation is prohibited.
    c. Access to RCS issued student email accounts is a privilege granted to students and may be revoked or withheld at the discretion of the RCS administration, faculty or staff.
    d. Students shall not attempt to read, delete, copy, or modify the email of any other user.
    e. Students shall not deliberately interfere with the ability of other students or staff to send or receive email.
    f. Students shall not use the email system in a way that is contradictory with directions of teachers, other staff, and generally accepted network protocol.
    g. Students shall not respond to unsolicited email messages from any source without the permission of their supervising teacher.
    h. Students shall not receive or respond to email or on-line information that consists of obscene, suggestive, illegal, offensive, pornographic, or objectionable content. If any such material is received it shall be reported immediately to the supervising teacher or authorized RCS Department of Technology staff for action including deletion, tracking, and reporting to proper law enforcement authorities, if appropriate.
    i. Disciplinary Action: Use of the RCS issued email accounts contrary to this policy or in an illegal manner shall be subject to the loss of rights and possible disciplinary or law enforcement action.
12) Students may not connect personal devices to any RCS restricted network. Students may connect personal devices to the "RCS Public" wireless network.
13) Grade K-8 students may not use personal technology on campus or on field trips during regular school hours, except for the authorized use of a personal device for e-reading purposes or as specified in a Diocesan Learning Plan.
14) Grade K-8 students may use personal devices for e-reading purposes, but may have e-reading privileges revoked if any of the provisions are violated.

a. All e-reading devices must be registered with the school Technology Integration Specialist (TIS) and accompanied by the Agreement Form signed both by the parents and the student.
b. e-reading devices are to be used only for the reading of school approved material (books, etc.) and not for other purposes such as web surfing, communication, entertainment, music, gaming, etc.
c. All material on the e-reading device must comply with the spirit and policies of Rochester Catholic Schools.
d. e-reading devices must be used at appropriate times in accordance with teacher instructions. The device must not be a distraction for the student or those around him/her nor be a source of any classroom disruption.
e. The student is responsible for knowing how to properly and effectively use their e-reading device.

15) Grade 9-12 use of mobile phones: Mobile phones have become an integral tool for many parents to communicate with their son or daughter during the school day:
    a. Student use of mobile phones and portable/mobile electronic devices are permitted with the exception of the following locations: classrooms (unless explicit permission is granted by the instructor), computer lab, auditorium, and quiet study.
    b. The use of mobile phones and portable electronics is a great privilege. Students must exercise responsibility, maturity, and respect for others. Administration and staff reserve the right to revoke privileges from students who are found using mobile phones or portable devices to isolate, harass, disrupt, disrespect, cheat, or violate other policies and procedures set forth throughout this document or the student handbook.
16) Educational Applications and Programs: RCS may utilize computer software applications and web-based services that are operated by third parties. In order for our students to utilize these services, the service provider often requests the student's personal information in the form of their name and email address.

    Under the federal Children's Online Privacy Protection Act (COPPA), the law permits RCS to consent to the collection of personal information on behalf of all of its students. Prior to use of these educational applications or programs, the district will review "terms of use," "terms of service," and/or "privacy policy" to ensure that it will not compromise students' personally identifiable information, safety, and privacy.

    These services include G Suite for Education and other similar educational programs. A complete list of the programs may be viewed on the RCS website.

17) Consequences of Technology Misuse:
    a. Students may lose computer privileges from one week to a year, depending on the severity of the infraction. If student computer privileges are lost or restricted, it is the student's responsibility to make arrangements to complete assignments outside of school or in a highly supervised environment. Students may also be required to pay the cost of repairing or replacing damaged software and/or hardware due to the infraction. Multiple infractions will be subject to additional disciplinary action because repeat infractions are a form of insubordination.
    b. Students found using RCS or personal technology in a criminal manner will be immediately reported to the appropriate law enforcement agency. Parents of students will be notified as well, and suspension or expulsion from school may result depending on the severity of the offense.

C. Rules Specific to Rochester Catholic School Employees, Contractors and Volunteers:

1) RCS employees, contractors, and volunteers are allowed to use personal technology on campus provided it does not interfere with their roles and responsibilities.
2) When authorized by the building administrator, RCS volunteers are allowed to use RCS technology under the direct supervision of an RCS employee.
3) RCS employees in student supervisory roles are in part responsible for the students' actions on technology when under their supervision. RCS employees in student supervisory roles must be completely familiar with the RCS Technology Use Policy Student Procedures.
4) RCS employees or contractors needing to add or install additional software shall contact the Department of Technology for assistance after seeking approval from their building administrator. The Department of Technology must be consulted prior to the purchase of software to ensure the chosen software can be successfully deployed in our technology environment.
5) While RCS students are in the RCS school buildings, at RCS sponsored events or on field trips, employees are responsible for supervising and guiding student Internet use, and shall not leave students unattended while working on computers.
6) Employees, contractors, visitors, or guests may not attach (physically or via wireless) personal technology to RCS restricted networks. Employees, contractors, visitors, or guests may attach personal devices to the RCS Guest wireless network in accordance with the procedures for the guest wireless network in each building, or with the permission of the building administrator or Director of Technology. All staff and visitors may use the RCS Public wireless network.
7) RCS Employee Email and Messaging:
    - All email in the RCS email system is subject to monitoring; any email with purposes not related to RCS business and education must be limited as to not interfere with the employee's' roles and responsibilities.
    - RCS employees are asked not to provide their RCS email address for non-work related correspondence or contacts. Any personal email in the RCS email system shall reflect an ethical and professional image that is consistent with RCS standards.
    - RCS staff should not use the RCS email system, web document repository or network drives for storage of personal information or files, including personally owned videos, music, or photographs.
    - Personal use of RCS email for the purpose of forwarding spam, jokes, chain letters, and third-party solicitations to RCS or external email recipients is prohibited.
    - Submitting solicitations, public announcements, or invitations to personal sales events, such as Pampered Chef, Stamping-Up, Mary Kay, etc., is subject to approval by your building administrator, and shall not be sent system-wide, or to major RCS mailing lists.

- The use of Instant Messenger (IM) software, such as Google Hangouts Chat, is limited to professional and internal communication only.
- Personal web-based email accounts shall be used only when appropriate. RCS is not responsible for external email networks.
- Since RCS email can contain student private data or other RCS private information, care must be taken to protect it, especially when accessed or stored on mobile devices which could be lost or stolen.
- Employees or contractors may only use RCS authorized cloud data services to sync RCS owned data. The utmost care must be taken to protect the data. Student private data must be protected, and only the minimum amount of data should be included which is required to complete necessary RCS work related tasks. Employee or contractor owned personal mobile devices or home computer accounts and their data folders must be protected with a non-trivial password or PIN, which must not be shared with other individuals. If a personal mobile device or home computer account storing RCS data is lost, stolen or otherwise compromised, the employee or contractor must immediately contact the appropriate RCS building administrator and Director of Technology.
- All RCS employees who have access to RCS technology, and have been provided an email address, shall check their email account at least once per working day for bulletins and pertinent information.

8) RCS employees are responsible for securing a backup of their important computer work preferably through the use of Google Drive on an RCS G Suite for Education account.
9) Faculty and support staff that are required to maintain a web page must review their online content and make necessary updates at least once per week.
10) RCS owned mobile devices issued to faculty and staff including but not limited to, laptops, tablets, cell phones, iPads, etc. are:
    - Professional tools provided to faculty/staff to support functions associated with employment expectations;
    - Very likely to have RCS student private data in the device storage.

    Therefore any RCS owned mobile device shall not be handled or used by any person(s) other than the intended RCS employee. RCS staff unmanaged mobile device guidelines: The following rules apply to RCS owned mobile devices:
    a. RCS mobile device return procedure: Individual RCS owned devices and accessories must be returned to the RCS Department of Technology upon request or upon termination of employment of contract. If an RCS employee, contractor or volunteer fails to return the RCS owned mobile device, that individual may be subject to criminal prosecution or civil liability. The individual will also pay the replacement cost of the RCS owned device. Furthermore, RCS employees, contractors, or volunteers will be responsible for any damage to the RCS owned device, and must return the RCS owned device and accessories to the RCS Department of Technology in satisfactory condition.

b. RCS employees may install personally owned iPad apps to their RCS issued iPads, provided the apps are beneficial for their RCS business or educational needs and do not interfere with their professional duties or the intended purpose of the device.
c. Taking care of your RCS owned mobile device: RCS employees, contractors, and volunteers are responsible for the general care of the mobile device they have been issued by the district.
    - Only use a clean, soft cloth to clean the screen; do not use cleansers of any type.
    - Cords and cables must be inserted carefully into the device to prevent damage.
    - Devices must remain free of any writing, drawing, stickers, or labels that are not the property of RCS.
    - Devices must never be left in an unlocked car or any unsupervised area.
    - Devices that are broken or fail to work properly must be immediately taken to the RCS Technology office for an evaluation of the equipment.
d. Understanding Backup and Data Ownership: Any RCS unmanaged mobile device in your possession may not have a managed backup for your data. It is your sole responsibility to back up any valuable data on these devices, as they may be wiped, crash, or be lost / stolen at any time. Any data stored on these devices is the property of RCS, and may be copied, removed, or modified at any time. Personal data storage on RCS owned devices must be strictly limited to the business operation of the device. Any personal data stored on RCS devices will become property of RCS.
e. Protection of Student Private Data: RCS staff is responsible for the protection of RCS Student Private Data. RCS staff should avoid storing any student private data in the memory or storage of unmanaged mobile devices so that it cannot be compromised should the device be lost or stolen. Staff shall instead use RCS managed computers or approved web applications, such as Infinite Campus, to store and manipulate student private data.
f. Loss of the Device: Should an RCS owned unmanaged mobile device be lost or stolen, the staff member shall immediately notify their building administrator and the RCS Department of Technology.

11) Consequences of Technology Misuse:
- RCS employees or contractors misusing RCS technology or personal technology on or off campus are subject to disciplinary measures deemed appropriate by their building administrator.
- Volunteers misusing RCS technology or personal technology on campus will be asked to cease and leave immediately, and may forfeit their volunteer privileges and/or access to RCS buildings.
- RCS employees, contractors, volunteers, or guests found using RCS technology in a criminal manner will be immediately reported to the appropriate law enforcement agency.

Rochester Catholic Schools Technology Use Agreement for RCS Students

I understand that the Rochester Catholic Schools (RCS) provides computer technology equipment, software, and Internet access for educational purposes. Use of computer technology is a privilege that requires responsibility.

Should I violate the rules as stated in the RCS Technology Use Policy, or participate in unethical behavior when using the computer technology, my access will be limited or revoked. Other school disciplinary action such as suspension and/or expulsion from school may also be taken depending on the severity. Criminal behavior will result in legal action with the appropriate Law Enforcement Agencies.

I have read, understand and agree with the Technology Use Policy of the Rochester Catholic Schools. I agree to review updates to the RCS Technology Use Policy that will be provided at the beginning of each school year.

Student:

Date: _____

Last Name (print): _____ First Name (print): _____

Signature: _____ Grade: _____

Parent/Guardian:

Date: _____

Last Name (print): _____ First Name (print): _____

Signature: _____

If registering an elementary e-reading device only:

Make/Model

_____