

### Acceptable Computer System Use

The School Board provides a computer system, including the Internet, to promote educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart telephones, the Internet and other internal or external networks.

All use of the Division's computer system must be (1) in support of education and/or research, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Any communication or material generated using the computer system, including electronic mail, instant or text messages, tweets, or other files deleted from a user's account, may be monitored or read, and/or archived by school officials.

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the computer system. The procedures shall include:

- (1) a prohibition against use by Division employees and students of the division's computer equipment and communications services for sending, receiving, viewing or downloading illegal material via the Internet;
- (2) provisions, including the selection and operation of a technology protection measure for the division's computers having Internet access to filter or block Internet access through such computers, that seek to prevent access to
  - (a) child pornography as set out in Va. Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
  - (b) obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and
  - (c) material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;
- (3) provisions establishing that the technology protection measure is enforced during any use of the Division's computers;
- (4) provisions establishing that all usage of the computer system may be monitored;
- (5) provisions designed to educate students and employees about appropriate online behavior, including interacting with students and other individuals on social networking websites, blogs, in chat rooms and cyberbullying awareness and response;
- (6) provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful activities;
- (7) provisions prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- (8) a component on Internet safety for students that is integrated in the division's instructional program.

Use of the School Division's computer system shall be consistent with the educational or instructional mission or administrative function of the Division as well as the varied instructional needs, learning styles, abilities and developmental levels of students.

The Division's computer network system is not a public forum.

© 5/13 VSBA

RADFORD CITY PUBLIC SCHOOLS

Each teacher, administrator, student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement, GAB-E1/IIBEA-E2, before using the Division's computer system. The failure of any student, teacher or administrator to follow the terms of the Agreement, this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

The School Board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The school board will review, amend if necessary, and approve this policy every two years.

Adopted: October 22, 2011 RCPS

Revised March 22, 2016

---

---

Legal Refs: 18 U.S.C. §§ 1460, 2256.  
47 U.S.C. § 254.

Code of Virginia, 1950, as amended, §§ 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2, and 22.1-78.

Cross Refs.:	GCPD	Professional Staff Members: Contract Status and Discipline
	GDPD	Support Staff Members: Contract Status and Discipline
	JFC	Student Conduct
	JFC-R	Standards of Student Conduct

## ACCEPTABLE COMPUTER SYSTEM USE

All use of the Radford City School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart phones, the Internet and any other internal or external network.

### Computer System Use-Terms and Conditions:

1. **Acceptable Use.** Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or (2) for legitimate school business.
2. **Privilege.** The use of the Division's computer system is a privilege, not a right.
3. **Unacceptable Use.** Each user is responsible for his or her actions on the computer system. Prohibited conduct includes but is not limited to:
  - using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any federal, state, or local law.
  - sending, receiving, viewing or downloading illegal material via the computer system.
  - unauthorized downloading of software including gaming software.
  - using the computer system for private financial or commercial purposes.
  - wastefully using resources, such as file space, and network bandwidth.
  - gaining unauthorized access to resources or entities by misuse of security credentials.
  - posting material created by another without his or her consent.
  - submitting, posting, publishing, or displaying any obscene, profane, threatening, illegal, or other inappropriate material including defaming another person's character.
  - repeated defamation of individuals or a group by means of intimidation, harassing, or coercing is categorized as cyberbullying.
  - using the computer system while access privileges are suspended or revoked.
  - theft of computer system or components comprised of
  - vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.
  - threatening illegal or immoral acts.
  - plagiarism constitutes a violation of the law and district policy.
  - using a cell phone, portable device or other similar electronic device to distribute pictures or videos of sexually explicit images, referred to as "sexting".
4. **Network Etiquette.** Each user is expected to abide by rules of etiquette, including the following:
  - be polite.
  - users shall not forge, intercept or interfere with electronic mail messages.
  - use appropriate language. The use of obscene, lewd, profane, lascivious, threatening or disrespectful language is prohibited.

- users shall not post personal information other than directory information as defined in Policy JO Student Records about themselves or others.
  - users shall respect the network/Internet resource limits. Network bandwidth is a finite resource
  - users shall not post chain letters or download large files.
  - users shall not use the computer system to disrupt others or employ hacking techniques.
  - users shall not modify or delete data owned by others. All data created for use in RCPS, is therefore owned by RCPS and cannot be removed without explicit permission.
5. **Liability.** The School Board makes no warranties for the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs, or damages incurred to the School District relating to or arising out of any violation policies and procedures. In the relationship of 3<sup>rd</sup> party accidental damage insurance either purchased by the user or School District, the user shall compensate RCPS for damages or deductible not covered by policy.
6. **Issued Technology Equipment.** Equipment can only be issued to the recipient after signing Equipment Loan Form or the Chromebook Use Agreement. Issued technology equipment remains property of Radford City Public Schools unless otherwise released. Issued equipment will follow the guidelines set forth by the Equipment Loan Form or the Chromebook Use Agreement.
7. **Security.** Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. This includes violations by students while monitored by teaching staff. All users shall keep their passwords confidential and shall follow computer virus protection procedures.
8. **Vandalism.** Intentional destruction of or interference with any part of the computer system through creating or downloading computer viruses or by any other means, including physical damage is prohibited and should be referred to in the liability section of the AUP regulation.
9. **Charges.** The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone or long-distance charges. Employees may be responsible for replacing or repairing lost or damage devices, refer to the liability section of the AUP regulation.
10. **Electronic Mail.** The School Division's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff in fulfilling their duties and as an education tool. Electronic mail is not private. Students' electronic mail will be monitored. The electronic mail of staff may be monitored and accessed by the School Division. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users shall be held personally liable for the content of any electronic message they create. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.

11. **Enforcement.** Software or systems will be installed on the division's computers or network to filter or block Internet access and protect the users from pornography, obscenity, and other potentially harmful websites. The online activities of users may also be monitored manually and any violation or attempts to circumvent these protective measures shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.
12. **Internet Safety.** Internet exploration opens a world of possibilities for students, expanding their horizons and exposing them to various cultures and different ways of life. The service however, can be a source of dangers if it is used inappropriately. The full version of the RCPS Technology Safety Guidelines can be found at <http://www.rcps.org>.
13. **Cloud Computing.** Radford City School Division is utilizing "cloud computing" to support staff learning through collaboration. "Cloud computing" allows staff to access certain computer programs, services, and files not hosted by Radford City School Division from anywhere there is an Internet connection. Radford City School Division is not responsible for intermittence or loss of data. Staff members are expected to use these services in a professional manner. Username and demographics of a student may be created on 3<sup>rd</sup> party databases and websites for use in educational instruction. The accounts created on 3<sup>rd</sup> party websites are not under the complete control of RCPS.
14. **Personal Use.** Personal use of technology resources must not interfere with the employee's job performance. Staff shall not use School Division technology systems for soliciting, proselytizing, advocating or communicating the views of an individual or non-school sponsored organizations. Division employees may not abuse their access to technology resources.
15. **Web-based Posting and Social Networking.** Occurs through various websites that allow users to share content, interact and develop communities around similar educational interests.
  - Let your administrator, IT Department, fellow teachers and parents know about your educational network.
  - When available, use school-supported networking tools.
  - Have a clear statement of purpose and outcomes for the use of the networking tool.
  - Establish a code of conduct for all network participants.
  - Pay close attention to the site's security settings and allow only approved participants access to the site.
  - Web posting and Social Networking are first and foremost a tool for learning, and as such will sometimes be constrained by the various requirements and rules of classroom teachers. Students are welcome to post on any school-appropriate subject or site.
  - All postings will be viewed by members outside the RCPS School District, and any inappropriate posting/speech should be reported to teachers or school administration immediately.

Adopted: April 7, 2005.

---

Revised:      May 27, 2008.  
                  October 11, 2011 RCPS  
                  January 10, 2013 RCPS  
                  March 8, 2016 RCPS