

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, optical media devices, tape drives, servers, mainframe and personal computers, 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 used on the computer system, including electronic mail or other files deleted from a user's account, may be monitored or read 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 by minors;
- (4) provisions establishing that the online activities of minors will be monitored;
- (5) provisions designed to protect the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- (6) provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful activities by minors online;
- (7) provisions prohibiting the unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- (8) a component of 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 system is not a public forum.

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 Division Superintendent shall submit to the Virginia Department of Education this policy and accompanying regulation biennially.

Adopted: April 7, 2005.

Revisions Approved: July 6, 2006.

May 27, 2008.

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.

ACCEPTABLE COMPUTER SYSTEM USE POLICY

The Radford City School Board provides a computer system, including access to the Internet, wired or wireless, to promote educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes hardware, software, data communication lines and devices, personal communication devices, terminals, printers, optical media devices, tape drives, servers, wireless devices, laptops and personal computers, the Internet and other internal or external networks.

Student Use

Radford City Schools operates under a “parent consent” policy for students regarding internet access. This means that students must have a written parent/guardian permission form on file at the school before they will be allowed access to the internet through any school computer. It must be understood that while accessing the internet through a computer owned or leased by Radford City Schools, all students will be expected to adhere to the division’s Acceptable Computer Use Policy. At this time, the school division does not provide students with email accounts, nor does it allow students’ access to internet web mail clients or services, instant messaging, or chat rooms.

Appropriate use of computers by students is closely monitored by the classroom teacher and principal. If a student uses a computer inappropriately, as deemed by the classroom teacher and administrator, he/she will lose computer privileges for a period of time. Examples are as follows, but are not limited to: Inappropriate messages, non-teacher directed chat rooms, suggestive messages/sites, sharing passwords, chain e-mail, threatening messages, pornographic sites, illegal activities, hacking activities, violence and hate, trespassing, plagiarism, spamming, personal financial gain, vandalism, using illegal copies of copyrighted software.

The use of communication technologies (school or personally owned equipment), such as email, cell phone and pager text messages, instant messaging and defamatory personal websites to facilitate deliberate, repeated and hostile behavior by an individual or group toward another (cyberbullying) will not be tolerated. All instances of cyberbullying, whether on school property or not, will be investigated. Students may be disciplined for participation in such inappropriate activities even if the offense occurs off of school grounds.

Employee Users

For staff users, the school district’s computer system must be used for education related purposes and performance of the employee’s job duties. Incidental personal use of school computers is permitted for employees so long as such use does not interfere with the employee’s job duties and performance, with system operations, or with other system users. Personal use must comply with this policy and all other applicable school district policies, procedures and rules contained in this policy. Personal use must also comply with applicable local, state and federal laws; and must not damage the school district’s computer system.

The school district must protect its computer system against numerous external and internal risks and threats. Users are critical players in protecting these school district assets and in lessening risks that can destroy these important resources. Consequently, employees are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Director of Technology or designee.

For employees who are provided cell phones/PDAs for work purposes, all provisions of the policy also apply to these devices.

Acceptable Use

All use of the division’s computer system must be (1) in support of education and/or research, (2) educational activities or (3) for legitimate school business. Access to the school district’s computer system through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the school district, which reserves the right to deny access to prevent further

unauthorized, inappropriate or illegal activity. The school district may revoke those privileges and/or administer appropriate disciplinary action. The school district will cooperate to the extent legally required with the local, state and federal officials in any investigation concerning or related to the misuse of the system.

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the computer system, including the prohibition of illegal material, prevention of access to material that the school division deems to be harmful to juveniles as defined in Va. Code sections 18.2-390 and measures to enforce this policy and regulation, including the selection of an internet filtering system applied to all of the division's computers having internet access. This system is designed to filter and to block Internet access through such computers to child pornography as set out in Va. Code section 18.2-374.1.1 and obscenity as defined in Va. Code section 18.2-372. Any communication or material used on the computer system, including electronic mail or other files deleted from a user's account may be monitored or read by school officials.

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 network and the division's internet connection may not be used to access, download, store, and/or distribute any material (text, graphic, photo, or audio) which is defamatory, abusive, obscene, profane, threatening, or sexually explicit. The Division's computer system is not a public forum.

Each teacher, administrator, student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement, GAB- E1/IIBEA-E1, 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.

Liability

Radford City Schools makes no warranties of any kind, expressed or implied, for internet service. Use of any information obtained via the internet is at each user's risk. The division specifically denies any responsibility for the accuracy or quality of information obtained through the internet.

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 Division Superintendent shall submit to the Virginia Department of Education this policy and accompanying regulations as required.

General Guidelines

School district guidelines on plagiarism will govern use of material accessed through the school district's computer system. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

All software used on school district computers will be coordinated through the Director of Technology or designee.

It is the responsibility of each staff member to take the necessary precautions to protect all school district computer equipment from loss by damage, theft or misplacement.

Any computer equipment that is damaged, stolen or misplaced must be reported immediately to the Director of Technology or designee so that warranty status can be determined and appropriate authorities can be notified when necessary. Failure to report lost or damaged equipment will be construed as an attempt to conceal the loss of, or damage to, the equipment and can result in the user being held financially liable or subject to disciplinary action.

Computer equipment that is damaged, stolen, or misplaced that is not covered under warranty is the obligation of the staff member's department or school, and arrangements for replacement will be the joint responsibility of the department head or principal and the Director of Technology or designee.

It is often necessary to access user accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and to store for archival purposes, any user accounts or communications for any reason in order to uphold this policy and to maintain the system. All emails and instant messages sent through the school district network are subject to logging and archiving. Users have no privacy expectation in the contents of their files or any of their use of the school district's computer system. The school district reserves the right to monitor, track, log, and access the systems use and to monitor and allocate files server space.

The school district reserves the right to restrict access to any internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the school district uses technology protection measures that block or filter inappropriate material on the internet. Measures designed to restrict student or staff access to harmful material may be disabled to allow staff members to do research or for other lawful purposes. Disabling filtering/blocking mechanisms must be approved through the Director of Technology or designee.

The use of the school district's computer system for illegal, inappropriate, unacceptable or unethical purposes is prohibited. Violations as described in this policy may be reported to the school district administration and to appropriate legal authorities. The school division will cooperate with authorities to the extent legally required in all investigations.

Laptop computers are available for student checkout on a limited basis. Additionally, each instructional staff member in the division is provided a tablet PC to be used for school business. Repairs that become necessary due to unauthorized installation of software or reconfiguring of the computer may result in a fee being charged to the assigned user.

In schools where laptops are available for student/staff checkout, the ITRT will be responsible for establishing guidelines for the timely return of the computer or peripheral device.

Users should be aware that the viewing of streaming video or television broadcasts will slow down the network for other users. This practice is strictly prohibited unless it is related to the education of the division's students or required of a staff member to perform his/her job duties.

Internet Conduct

Users will abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Use appropriate language. Use of vulgar language does not conform to the established code of student conduct and may result in disciplinary action. Employees are also expected to abide by generally accepted professional standards of conduct.
- Illegal activities and use of the internet in furtherance of illegal activities are strictly forbidden.
- Use of the internet for financial gain via district owned equipment is strictly forbidden.

Unacceptable Use

All users (employees, students or guests) are responsible for his or her actions on the computer system.

Prohibited conduct includes:

- Install, distribute, reproduce or use copyrighted software on school district computers, or copy school district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. This includes loading or using of software, hardware or peripheral devices on a computer without permission.
- Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer, electronic communication systems, or network services, whether wired, wireless, cable or by other means.
- Altering or attempting to alter any school district computing or networking components without authorization or beyond one's level of authorization.
- Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other game or games of chance.
- Engage in commercial, for profit, or any personal business purposes unless permitted by district policy.
- Accessing, attempting to access or modifying computer files, the computer system or computer networks without authorization. This includes using another user's password with or without the consent of the user. Users will be held responsible for the result of any misuse of the user name or password while the users' system access was left unattended and accessible to others, whether intentional or through negligence.

Also includes: attempting to bypass the security system; copying, renaming, changing, examining, or deleting files belonging to someone else without the owner's permission; interfering with the work of others; crashing or attempting to crash the system; damaging, modifying, altering, destroying or copying computer files or resources; and subverting or attempting to subvert the restrictions associated with the district's or school's network or files.

- Copying or accessing the files of another user for the purpose of copying the contents and representing it as his or her own work.
- Intimidate or harass another individual.
- Violate the privacy, security or confidentiality of information, including but not limited to student data.
- Political lobbying
- Accessing or participating in "chat rooms", including but not limited to social networking sites such as My Space, Facebook, and Xenga.
- Viewing web casts with no related educational value or association with an employee's job duties.
- Using school system web page server to store personal items or linking to personal business

Because electronic information is so volatile and easily reproduced, respect for the work and personal expression of others is especially important in computer environments. Violations such as plagiarism, invasion of privacy, unauthorized access, and copyright violation are grounds for disciplinary action.

United States copyright and patent laws protect the interest of authors, inventors and software developers and their products. Software license agreements serve to increase compliance with copyright and patent laws, and to help ensure publishers, authors, and developers a return on their investments. It is against federal law to violate the copyrights or patents of computer software developers.

Consequences of Inappropriate Use

General rules for behavior apply when using the school division computer system. Users must be aware that violations of this policy or other policies, or unlawful use of the computer system may result in loss of computer access, and a variety of other disciplinary actions applicable to all users. This policy incorporates all other relevant school division policies.

The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damages resulting from willful or deliberate violations of this policy.

Internet Safety

While on line exploration opens a world of possibilities for students, expanding their horizons and exposing them to various cultures and ways of life, they can also be exposed to dangers as they explore the information highway. There are individuals who attempt to sexually exploit children through the use of on-line services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts. These individuals are often willing to devote considerable amounts of time, money, and energy in this process. These individuals attempt to gradually lower children's inhibitions by slowly introducing inappropriate content into their conversations.

Radford City Schools operates a private network for students, teachers, and staff with a secure connection to the Internet. Network security is maintained through the combined use of an Internet Filtering Appliance, a firewall, staff guidelines and an acceptable use policy. The following information demonstrates that Radford City Schools is in compliance with the Children's Internet Protection Act (CIPA) and 22.1-70.2 of the Code of Virginia.

The RCPS firewall was updated in 2008. The firewall prevents unauthorized intrusion and access to school system resources by producing a physical barrier between the Radford City School's private network and the Internet. The firewall permits outbound traffic from the Radford City School's private network to Internet.

The Internet filtering appliance was updated in 2008. This filter prevents access to harmful and illegal materials by users of the Radford City School's network. The server is updated automatically each day and new definitions are applied by the product provider to ensure that it continues to stay current on materials that must be blocked to protect minors. The filtering appliance enables the staff of Radford City to track and monitor online activities. The software also filters and controls chat rooms, pornography, instant messaging, and other potentially harmful forms of electronic communication. In addition, RCPS installed in 2005 and updated in 2008, the email spam filter.

Internet Safety training will be required annually for all Radford City School students. This training will also be offered to teachers, parents, and members of the Radford community. This training will follow the guidelines established by the Virginia Department of Education as directed by HB58 adopted March 2006.

Staff Guidelines for the use of Instructional Technology were adopted by the Radford City School Board in 2000. These guidelines establish procedures that protect the faculty and staff from harmful materials and practices that may result from the use of technology in the work place.

The Radford City School Board first adopted an Acceptable Use Policy in 2001. The Board has since revised its Acceptable Use Policy in 2005 and again in 2006.

Student violations of the Acceptable Use Policy are subject to discipline procedures under the RCPS student code of conduct. The full version of the RCPS Acceptable Use Policy can be found at

<http://www.rcps.org>.

Adopted: April 7, 2005.

Revised: May 27, 2008.

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: JFC Student Conduct
JFC-R Standards of Student Conduct

ACCEPTABLE COMPUTER SYSTEM USE AGREEMENT

Each student and his or her parent/guardian must sign this Agreement before being granted use of the School Division's computer system. Read this Agreement carefully before signing.

Prior to signing this Agreement, read Policy and Regulation GAB/IIBEA, Acceptable Computer System Use. If you have any questions about this policy or regulation, contact your student's principal.

I understand and agree to abide by the School Division's Acceptable Computer System Use Policy and Regulation. I understand that the School Division may access and monitor my use of the computer system, including my use of the internet, e-mail and downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or Regulation, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Student Signature _____

Date _____

Student Name _____

(Please Print)

I have read this Agreement and Policy and Regulation GAB/IIBEA. I understand that access to the computer system is intended for educational purposes and the Radford City School Division has taken precautions to eliminate inappropriate material. I also recognize, however, that it is impossible for the School Division to restrict access to all inappropriate material and I will not hold the School Division responsible for information acquired on the computer system. I have discussed the terms of this agreement, policy and regulation with my student.

I grant permission for my student to use the computer system and for the School Division to issue an account for my student.

Parent/Guardian Signature _____

Date _____

Parent/Guardian Name _____

(Please Print)

ACCEPTABLE COMPUTER SYSTEM USE AGREEMENT

Each employee must sign this Agreement as a condition for using the School Division's computer system. Read this Agreement carefully before signing.

Prior to signing this Agreement, read Policy and Regulation GAB/IIBEA, Acceptable Computer System Use. If you have any questions about this policy or regulation, contact your supervisor.

I understand and agree to abide by the School Division's Acceptable Computer System Use Policy and Regulation. I understand that the School Division may access and monitor my use of the computer system, including my use of the internet, e-mail and downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or Regulation, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Employee Signature _____

Date _____

Employee Name _____

(Please Print)