

## **Policy IBEA**

### **Acceptable Computer Use Policy**

The Radford City 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 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. 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 a technology for the division's computers having Internet access to filter or 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 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, IBEA-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 regulations biennially.

## Policy IBEA-R

### Acceptable Computer System Use

All use of the Radford 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 drives, servers, mainframe and personal computers, 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 education 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:
  - Using the network for any illegal activity, including violation of copyright or other 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
  - Downloading copyrighted material for unauthorized use
  - Using the computer system for private financial or commercial gain.
  - Wastefully using resources such as file space.
  - Gaining unauthorized access to resources or entities.
  - Posting material authorized or created by another without his or her consent.
  - Using the computer system for commercial or private advertising.
  - Submitting, posting, publishing or displaying any obscene, profane, threatening, illegal or other inappropriate material.
  - Using the computer system while access privileges are suspended or revoked.
  - Vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.

#### Clarification of Unacceptable Computer Use

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, 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.

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.

Security systems for computers exist to ensure that the computers and systems are functional for all users. User responsibility is the ultimate safeguard against misuse. Misuse includes, but is not limited to, the following examples:

- Accessing or attempting to access computer files, the computer systems, or computer networks without authorization.
  - Damaging, modifying, altering, destroying or copying computer files.
  - Modifying or attempting to modify computer systems or facilities.
  - Tampering with terminals or any other associated equipment.
  - Crashing or attempting to crash the system.
  - Subverting or attempting to subvert the restrictions associated with the district's or school's networks or computer files.
  - Taking possession of a computer, peripheral device or any other property.
  - Intentionally wasting, abusing and/or damaging computer resources.
  - Intentionally interfering with the work of other users.
  - Violating confidentiality, copyrights or license agreements.
  - Unauthorized use of a password.
  - Attempting to bypass the system security.
  - Copying, renaming, changing, examining, or deleting files belonging to someone else without the owner's permission.
  - Copying or accessing the files of another user for the purpose of copying the contents and representing it as his or her own work. (This is interpreted as plagiarism.)
  - Loading software on a computer without permission.
4. Network Etiquette. Each user is expected to abide by generally accepted 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, threatening or disrespectful language is prohibited.
  - Users shall not post personal contact information about themselves or others.
  - Users shall respect the computer system's resource limits.
  - Users shall not post chain letters or download large files.
  - Users shall not use the computer system to disrupt others
  - Users shall not read, modify or delete data owned by others.
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 by the School Board relating to or arising out of any violation of these procedures.

6. 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. All users shall keep their passwords confidential and shall follow computer virus protection procedures.
7. Vandalism. Intentional destruction of any part of the computer system through creating or downloading computer viruses or by any other means is prohibited.
8. 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.
9. 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 educational tool. Electronic mail is not private and 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.
10. Enforcement. This procedure and the policy it supports shall be enforced by monitoring information on the School Division's computer system. To protect students, software will be installed on the division's computers having Internet access to filter or block internet access through such computers to child pornography as set out in Va. Code 18.2-374.1:1 and obscenity as defined in Va. Code section 18.2-372 and may be installed on the computer system to block other obscene/illegal material as well as material that the school division deems to be harmful to juveniles. Any violation of these regulations 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.
11. 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 established code of student conduct and may result in disciplinary action.
  - 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 also strictly forbidden.

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. 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 a student 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 installed in 1998. 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 deployed in 2000. 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 student activities. The software also filters and controls chat rooms, pornography, instant messaging, and other potentially harmful forms of electronic communication.

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. The RCPS Acceptable Use Policy covers topics on student use of technology that includes:

- Accessing of obscene or inappropriate materials.
- Student use of obscenity or profanity on a computer or network.
- Restrictions on students regarding the dissemination of personal information.
- Unlawful student activities and conduct on the Internet.

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>.

**Acceptable Use Policy (AUP) and Computing Rules  
Radford City Schools**

1. Users must not attempt to penetrate any school computing system security or the security system of off-campus organizations.
2. Users must not intentionally locate, write, send, or store material that is lewd, obscene, or pornographic.
3. Users must abide by system regulations posted in the computer laboratories and by any other rules established by faculty in regard to computer use.
4. The user is responsible for all activity that occurs under his or her account. Passwords must not be shared.
5. The user must abide by all copyright laws applicable to software, Internet materials, and other resources.
6. Radford City Schools' computing facilities may not be used for any commercial or business activity unless expressly authorized in writing by the school administration.
7. Users must not intentionally cause the computer or system to behave atypically.
8. Users may not intentionally gain unlawful access to others' files, programs, or accounts.
9. Users must use appropriate, inoffensive language in all electronic communications.
10. Users must not place unlawful information on the Internet nor use the Internet in any unlawful manner.

There are times when school personnel may need to examine files and actual or logged network sessions of a computer user. These times, though infrequent, are necessary for the reasonable and proper administration of school computing resources. At such times, school personnel are investigating violations or possible violations of security and /or rules and interactions that may be contributing to poor computer performance or computer malfunctions.

The Virginia Department of Education requires school divisions across the commonwealth to administer the Virginia Standards of Learning Tests each year. These tests are administered to students in grades 3, 5, and 8 as well as end of course tests in Algebra I, Algebra II, Geometry, World History I, World History II, US History, Earth Science, Biology, Chemistry, English 11 Reading and English 11 Writing. Beginning in the spring 2002 Radford City Schools will participate in the Virginia Standards of Learning on-line testing program. This program will provide students the opportunity to take the Virginia SOL test on the computer, which will provide a faster report of test data to school officials. Students testing on-line will access the test via the Internet through a secured site. Parents who choose not to allow their child to access the Internet through a computer at school are asked to give permission for their child to access the Internet for on-line testing purposes.

I agree to the rules and hereby give permission for \_\_\_\_\_ to use the computer and the Internet.

**Parent or Guardian Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

I agree to the above rules and will abide by them in my use of the computer and the Internet.

**Student Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

I do not wish for \_\_\_\_\_ to personally use the computers to access the Internet. I understand that the teacher, guidance counselors, lab assistants, may use the Internet in classroom instruction.

**Parent or Guardian Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

I do not wish for \_\_\_\_\_ to use the computer to access the Internet. I do however, grant permission for use of the computer for the Virginia Standards of Learning on-line testing program.

**Parent or Guardian Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_