RCPS ACCEPTABLE COMPUTER SYSTEM USE AGREEMENT
(POLICY 6.42)

The Internet is an electronic medium connecting computers and users all over the world. Students and teachers use the Internet as a learning tool to gather and evaluate information from multiple sources as well as to communicate and collaborate with individuals both within and outside the classroom. In the hands of skillful teachers who plan thoughtfully, technology is leveraged to transform lessons into engaging and purposeful learning experiences.

The School Board provides a computer system, as defined below, to catalyze the acquisition of knowledge and the development of 21st century skills: collaboration, communication, critical thinking, creativity, and citizenship. Technology and digital resources are powerful tools for engaging and purposeful learning, but they are tools that must be used responsibly and ethically within the school community. All users bear the responsibility of cultivating and enforcing the principles of digital citizenship when using technology and digital resources.

The term computer system includes, but is not limited to, hardware, software, online resources, network infrastructure, data, communication lines and devices, terminals, printers, CD, DVD and other media devices, flash drives, servers, computers, the Internet, mobile devices (both personal and school owned) and any other internal or external network. This includes any device that may be connected to or used to connect to the school division's network or electronically stored division material.

All use of the Division's computer system must be (1) in support of education or research and be consistent with the educational objectives of the Division, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Inappropriate use may result in cancellation of those privileges, disciplinary action, and/or legal action. Any communications or materials generated using the district network, including email, instant or text messages, social media posts, social networking, and other files, including communications and materials deleted from a user's account, may be monitored, read, and/or archived by division staff.

This policy applies to all users of the division's computer system. By using or accessing the computer system, the user agrees to abide by this policy and the Technology Use Guidelines established by the Superintendent.

The superintendent is responsible for establishing Technology Use Guidelines containing the appropriate uses, ethics and protocols for use of the computer system. It is the user's responsibility to know and follow this policy and the Technology Use Guidelines.

The Guidelines 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 digital citizenship, including interacting with students and other individuals on social networking websites and in chat rooms and cyberbullying awareness and response;
6. provisions designed to prevent unauthorized online access by users, including "hacking" and other unlawful online activities;
7. provisions requiring every user to protect the security of information necessary to access the computer system, such as usernames and passwords, and prohibiting the sharing of passwords;
8. provisions prohibiting the unauthorized disclosure, use, and dissemination of photographs and/or personal information of or regarding minors; and
9. a component on Internet safety for students that is integrated in the Division's instructional program.

Use of the School Division's computer system must 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.

Users of the division's computer system have no expectation of privacy for use of the division's resources or electronic devices including non-division owned devices while connected to division networks or computer resources.

Software and/or services may not be installed or downloaded on the division's computer system without the prior approval of the superintendent or superintendent's designee.

No employee or agent of the School Board or person or entity contracting with the School Board may download or use any application, including TikTok or WeChat, or access any website developed by ByteDance Ltd. or Tencent Holdings Ltd. (i) on any device or equipment issued, owned, or leased by the School Board, including mobile phones, desktop computers, laptop computers, tablets, or other devices capable of connecting to the Internet.

Each user of the division's computer system and a parent/guardian of each student user shall sign the Acceptable Computer System Use Agreement, before using the Division's computer system. The failure of any user 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 is not responsible for any unauthorized charges or fees resulting from access to the computer system.

Terms and Conditions

A. **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 for legitimate school business.

   Even though the purpose of using the computer system may be acceptable, such use may not occur in a manner that otherwise is in violation of School Board policy or administrative regulations.

B. **Privilege.** The use of the Division's computer system is a privilege, not a right.

C. **Unacceptable Use.** Each user is responsible for his or her actions on the computer system. Prohibited conduct includes but is not limited to:

1. 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;
2. sending, receiving, viewing or downloading illegal material via the computer system;
3. unauthorized downloading of software or files;
4. using the computer system for private financial or commercial gain;
5. wastefully using resources, such as file space;
6. gaining unauthorized access to resources or entities;
7. users should not attempt to bypass any form of security built into the system by Roanoke County Public Schools or attempt to access networks not specifically authorized for use.
8. posting material created by another without his or her consent;
9. submitting, posting, publishing or displaying any obscene, profane, threatening, illegal or other inappropriate material;
10. using the computer system while access privileges are suspended or revoked;
11. vandalizing the computer system, including destroying data by creating or spreading viruses or by other means;
12. computer users will not remove RCPS labels or tags nor will they alter the laptop's appearance. No substance, sticker, or adhesive material is to be placed on the computer.
13. intimidating, harassing, bullying, exploiting or coercing others;
14. threatening illegal or immoral acts;
15. capturing the image of someone else without his or her permission;
16. using mobile devices in restrooms or locker rooms;
17. using or impersonating the username and password of another user;
18. forging, intercepting, or interfering with email messages;
19. using the computer system to disrupt the learning or safety of others;
20. reading, modifying, or deleting data owned by others without their permission;
21. attempting to circumvent or interfere with administrative passwords and security measures or otherwise hacking into the computer system.

D. **Digital Citizenship.** Each user must abide by norms of digital citizenship including the following:

1. Users will be polite in all interactions.
2. Users will keep their username and password protected and will not share this information with others.
3. Users will always use appropriate language. The use of obscene, lewd, profane, threatening or disrespectful language is prohibited.
4. Users will not post personal information other than directory information as defined in Policy 7.09 (Student Records) about themselves or others.
5. Users will respect the computer system's resource limitations by not downloading or streaming content that may interfere with other users' access to the network.
6. Users will utilize the computer systems with proper procedures that ensure no harm to others or themselves.

E. **Mobile Devices Owned by the School Division.** The following specific regulations apply to mobile devices (portable devices including laptops) assigned to students for use both in and out of school. These regulations supplement those set forth in the Acceptable Use Policy (AUP) of the School Division's computer system:

1. All provisions of the Roanoke County Public Schools (RCPS) Acceptable Use Policy must be observed by students using mobile devices both in and outside of school.
2. ONLY authorized educational programs installed by RCPS staff may be used on RCPS Roanoke County mobile devices assigned to students.
3. Students will not stream games, music or download digital media unless directly related to classroom instruction.
4. Personal messaging is prohibited in school unless under the direct supervision of a teacher and for a classroom instructional purposes.
5. Students will not attempt to download, install, or use any software that is not authorized by RCPS.
6. Students may not remove or alter any part of the mobile device.
7. Students must handle and transport mobile computers responsibly; Mobile device must be in protective case while being transported.
8. Any damage determined by RCPS Technology staff to be intentional will be charged to the student (parts and labor up to the full replacement value of the computer).
9. Students will not remove RCPS labels or tags; students will not alter the laptop appearance; no substance is to be placed on the computer.
10. Students are responsible for keeping devices safe and secure. The student assumes the risk of loss, theft, destruction, or damage and is responsible for repair or replacement cost. Students must report loss or damage immediately.
11. District provided email and cloud storage will be available to students and must be used for instructional purposes.

F. **Use of Personal Mobile Devices.** Regulations regarding the use of personal mobile devices apply to use of such devices on school property or at school-sponsored activities.

1. Roanoke County Public Schools allows staff to connect privately-owned mobile electronic devices to the RCPS Staff BYOD network for educational or other school-related purposes.
2. RCPS stores the MAC address of mobile devices that access the RCPS Staff BYOD wireless network, however, no additional information is stored, monitored, or archived from staff personal mobile devices.
3. All provisions of the RCPS AUP and other relevant School Board policies and procedures and administrative regulations must be observed by staff using personal devices to the Staff BYOD wireless network. In addition, staff members should see School Board Policy 5.56 regarding Standards of On-Line Conduct for Employees.
4. The use of personal mobile devices is a privilege, not a right.
5. Personal mobile devices are brought to school at the student's and parents' own risk. RCPS is not responsible for loss, theft, damage, or other associated cost of any personal mobile device and students are responsible for securing their device at all times.
6. RCPS staff is not allowed to store, support, repair, or troubleshoot personal mobile devices.
7. No personal mobile device may be connected to the RCPS network via a cable. Staff network access is only provided via Wi-Fi access.
8. Wireless ad-hoc or peer-to-peer networking is prohibited.
9. Voice, video, or image capture applications may only be used with teacher or administrator permission.
10. The School Division reserves the right to inspect personal mobile devices and their content if reasonable suspicion exists that School Division policies or local, state, or federal laws have been violated.

G. **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.

H. **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.

I. **Vandalism.** Intentional destruction of any part of the computer system through creating or downloading computer viruses or by any other means is prohibited.

J. **Charges.** The school division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone, data, or long-distance charges.

K. **EMail.** The School Division's email system is owned and controlled by the School Division. The School Division may provide email to aid students and staff in fulfilling their duties and as an education tool. Email is not private. If students are given access to any type of email or communication system administered by Roanoke County Public Schools, such communications may be monitored. The email of staff may be monitored and accessed by the school division. All email may be archived. Unauthorized access to an email account by any student or employee is prohibited. Users may be held responsible and personally liable for the content of any electronic message they create or that is created under their account or password. 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.

L. **Enforcement.** Software will be installed on the Division's computers having Internet access to filter or block internet access through such computers to child pornography and obscenity. The online activities of users may also be monitored manually. 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.

Guidelines for Internet Safety

To ensure safety for all users of the Roanoke County Public Schools (RCPS) network, a comprehensive program of Internet Safety and Digital Citizenship is a critical element of the division's Acceptable Use Policy. CIPA compliant filtering systems are in place to minimize exposure to illegal or inappropriate information while on the Internet. Guidelines intended to ensure the safety of all are included in the policies for students and staff.

The following specific procedures exist to protect both employees and students utilizing the RCPS network:

1. All students and their parents are required to read and sign the AUP annually.
2. All staff members sign the AUP upon initial employment and when revisions are made to the AUP.
3. Parent meetings are held regularly to educate and inform parents of potential dangers both in and out of school. Written materials for parents are available via the RCPS web site. Potential dangers of which parents should be aware will be posted on the RCPS web site and in school newsletters.
4. A comprehensive program of Internet Safety and Digital Citizenship is in place in grades K-12 and will be reviewed annually. This program will be integrated into all curricular areas and updated as needed to provide adequate and timely instruction in all aspects of Internet Safety and Digital Citizenship. The program delineates the roles and responsibilities of all stakeholders.
5. A program of staff development will include annual review of these policies and curriculum by all professional staff as well as periodic updates via school-based meetings, web-based communications, and e-mail news regarding potential dangers or issues that should be addressed.