CENTERVILLE-ABINGTON COMMUNITY SCHOOL CORPORATION
STUDENT TECHNOLOGY RESPONSIBLE USE POLICY

All use of the Internet shall be consistent with Centerville-Abington School Corporation's goal of maximizing the potential of every person every day by facilitating resource sharing, innovation, and communication. Guidance and instruction will be provided and required for each individual granted Internet access through the school. The policy does not attempt to state all required and/or irresponsible behaviors by users. However, some specific examples are provided. The failure of any user to follow the terms of the Responsible Use Policy for Internet Access will result in the loss of privileges, disciplinary action and/or appropriate legal action. The signature(s) on the Permissions/Approval form is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance. *Note*: Students new to the school must attend for five consecutive days prior to getting their electronic device.

Internet Use- Terms and Conditions

1) Responsible Use - The use of your network account must be in support of education and research and be consistent with the educational objectives of Centerville Senior High School and Centerville-Abington Junior High School.

2) Privileges - The use of telecommunications services is a privilege, not a right. Inappropriate use will result in the cancellation of those privileges. The technology director and the school administrator will deem what is inappropriate use and their decision is final. The administration, faculty, and staff may request the technology director and/or the system administrators to deny, revoke, or suspend specific user accounts.

3) Nonresponsible Use – You are responsible for your actions and activities involving the network. Some examples of irresponsible use include but are not limited to:

- Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or state regulation.
- Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused.
- Downloading copyrighted material for personal use including music or videos.
- Using the network for private or commercial gain and/or using the network for commercial or private advertising.
- Gaining unauthorized access to resources or entities.
- Invading the privacy of individuals, including students and staff.
- Posting material authored or created by another without his/her consent.
- Posting anonymous messages.
- Accessing, submitting, posting/publishing or displaying defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing or illegal material, or any other material deemed educationally inappropriate.

- Using the network while access privileges are suspended or revoked.

4) Exclusive Use of Access - Network users are solely responsible for the use of their logins, passwords, and access privileges. Any problems that arise from the use of a registered user's login are the user's responsibility. The use of a registered login by someone other than the user is forbidden and is grounds for denial or limitation of network access privileges. Network resources can only be accessed with school owned computers, laptops and similar devices. Student owned computers, laptops, tablets, and other internet devices may not access CACS network resources either wirelessly or connected directly to the network. Students are encouraged to use personal thumb drives to backup, store and transport personal files between classrooms, home and school.

5) Network Etiquette – You are expected to abide by the accepted rules of network and safety etiquette. These include but are not limited to the following:

- Be polite.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- Do not reveal the addresses or telephone numbers of students or colleagues. Users may not post chain letters or engage in spamming.
- Do not disrupt the use of the network. All communications and information accessible via the network should be assumed to be property of CACS.

6) Personal Safety – For your own benefit, observe the following precautions:

- Do not post personal contact information about yourself or other people. This information includes, but is not limited to, your address, telephone number, work address, etc.
- Do not agree to meet with someone you have met online.
- Disclose to your teacher, librarian, or classroom supervisor any message you receive that is inappropriate or makes you feel uncomfortable.
- Do not let other students use your computer.

7) Search and Seizure/Due Process - Your network accounts are not private. Routine maintenance and monitoring of the email or file servers may lead to discovery that you have violated this policy or the law. The technology director and/or systems administrators will conduct searches if there is reasonable suspicion that you have violated this policy or the law, or if requested by local, state or federal law enforcement officials. CACS will cooperate fully with local, state, or federal officials in any investigation related to illegal activities conducted on network resources owned by Centerville-Abington Community School Corporation.

8) Security - Security on any computer system is of the highest priority, especially when the system involves many users. If you identify a security problem on technology resources, you must notify the technology director. Users should not demonstrate the problem to other users. Users should not use another student’s login information. Attempts to log on to the network with

a stolen identity or as a system administrator will result in cancellation of user privileges, suspension and/or possible expulsion. If a user is identified as a security risk or has a history of problems with other computer systems, CACS may deny access to technology resources.

9) Vandalism/Harassment – Vandalism and/or harassment will result in the cancellation of privileges, and disciplinary action will be taken. Vandalism is defined as any malicious and/or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to the uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent network security. Harassment is defined as the persistent annoyance of another user or the interference in another student's work. This includes, but is not limited to, the sending of unwanted e-mail.

10) Damage to the Computers: Intentional damage to the computers is not covered under any insurance or warranty. Damage deemed to be excessive or intentional will be paid in full by the person assigned to the computer. Accidental damages will be covered after a deductible of up to $100 is paid by the person assigned to the computer.

The student and parent(s)/guardian(s) need to sign the Responsible Use Policy each year while attending the Centerville-Abington Community School Corporation. By signing this agreement, you agree to abide by the rules and regulations outlined in the Student Technology Responsible Use Policy. **CACS reserves the right to amend this policy as needed.**

_____

(Student/ Date)

_____

(Parent-Guardian/ Date)