TECHNOLOGY USE GUIDELINES

All use of the Winchester Public 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 ("Computer System") includes, but is not limited to: hardware, software, data, communication lines and devices, terminals, display devices, printers, CD, DVD and other media devices, tape or flash drives, storage devices, servers, mainframe and personal computers, tablets, laptops, telephones (including cellular phones), cameras, projectors, multimedia devices, workstations, access to the internet or external drives, and other electronic services 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.

Computer System Use-Terms and Conditions:

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. All users are responsible for the safe, responsible, and educational use of the Computer System consistent with Policy IIBEA and these guidelines and are subject to state and federal law. The division's Computer System is not a public forum and is subject to Winchester Public Schools control.

General Use and Ownership.

- Winchester Public Schools proprietary information stored on electronic and computing devices whether owned or leased by Winchester Public Schools, the employee or a third party, remains the sole property of Winchester Public Schools.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Winchester Public Schools proprietary information.
- You may access, use or share Winchester Public Schools proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- For security and network maintenance purposes, authorized individuals within Winchester Public Schools may monitor equipment, systems and network traffic at any time.
- Winchester Public Schools reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Damage/Loss Responsibility. Users of Winchester Public Schools Computer System are expected to respect school property and be responsible in using the equipment. Users will follow all instructions regarding maintenance and care of the equipment. Winchester Public Schools is responsible for the routine maintenance or standard repairs to school-issued equipment. Users may be held responsible for the repair or replacement for intentional damage or lost or stolen equipment.

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

Acceptable Use. Each user is responsible for this or her own actions on the computer system. Examples of acceptable computer system use includes but is not limited to:

1.In accordance with teacher directives in the instructional setting, including:

- Research
- Organization of materials
- Brainstorming
- Composition
- Note-taking
- Instructional software and Internet activities
- Projects
- Correspondence
- Career Development
- Discussion Forums
- Electronic Collaboration

2.Comply with fair-use laws and copyright regulations while accessing the Internet:

- Understand, recognize, and respect the intellectual property of others;
- Present accurate information when collaboratively gathering or sharing information (e.g. avoid Wiki vandalism);
- Ethical gathering and/or presentation of information (e.g. avoid plagiarism, provide correct attribution, follow Creative Commons Law); and
- Cite all sources.

3.School-sponsored email:

- Use for legitimate WPS academic and curricular activities communications;
- Keep passwords and logins confidential and share them only with trusted adults;
- Only access your own account;
- Send messages that contain content in accordance with this policy and the Code of Student Conduct;
- Immediately report messages that violate this policy or the Code of Student Conduct to administration; and
- Download attachments only when user is certain the attachment is safe for the Computer System.

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.
- using the computer system for private financial or commercial purposes.
- wastefully using resources, such as file space, bandwidth, on-line time, or printing capacity.
- gaining unauthorized access to resources or entities.
- using the Computer System or the Internet to “hack” or gain unauthorized access to computers, networks, or information systems, including accessing another person’s account.
- use of anonymous proxies to circumvent content filtering.

- disabling filtering software or other technologies.
- posting material created by another without his or her consent.
- copying, downloading, or uploading another person's files which include personally identifiable information such as personal photos without that person's prior authorization.
- reading, altering, changing, block executing, or deleting files or communications belong to another use without the owner's express prior permission.
- submitting, posting, publishing, accessing, viewing, sending, sharing, downloading, or displaying any obscene, profane, sexually explicit, offensive, threatening, discriminatory, illegal, or other inappropriate material (including but not limited to unapproved executable video or audio files).
- using the computer system while access privileges are suspended or revoked.
- vandalizing the computer system, including destroying data by creating or spreading a worm, virus, malware, ransomware or other harmful or destructive form of programming or software.
- intimidating, harassing, bullying, or coercing others.
- using the Computer System for threatening illegal or immoral acts.
- effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee/student is not an intended recipient or logging into a server or account that the employee/student is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- port scanning or security scanning is expressly prohibited unless prior notification to Technology Department is made.
- executing any form of network monitoring which will intercept data not intended for the divisions host, unless this activity is a part of the employee's normal job/duty.
- circumventing user authentication or security of any host, network or account.
- revealing your account password to others or allowing use of your account by others.

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, 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 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 modify or delete data owned by others.
- recognize and honor the intellectual property of others by providing proper attribution to sources of work obtained, in whole or in part, from the Internet and, where required, obtaining the copyright owner's permission to use copyright-protected work.

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 is not responsible 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.

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.

Vandalism. Intentional destruction of or interference with any part of the computer system through creating or downloading computer viruses or by any other means is prohibited. Winchester Public Schools Computer System should be treated with care and all Computer Systems should be left in a good condition for the next user.

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.

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. All electronic mail may be archived. Unauthorized access to an electronic mail 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.

Photographs, Artwork, Videos, and Audio Materials. Photographs, artwork, videos and audio materials will be presented in such a way to protect the individual student. These materials may be used in newspapers, television, or the Winchester Public Schools website and social media pages only if the parent /guardian has approved the use.

Social Media. Social media includes Internet-based applications and mobile technologies that allow the creation and exchange of user-generated content. Examples of commonly used social media tools include, but are not limited to: blogs, message boards, chat groups, instant messaging, personal news updates, and music/video sharing (e.g., Facebook, Instagram, Snapchat, TikTok, Remind, YouTube, and Twitter). Users of the Winchester Public Schools Computer System may use social media on the school division' computer system only for educational purposes and only if allowed and accessible. Users may not attempt to circumvent the system to access social media platforms that are inaccessible.

Any use of social media must be in conformance with these Technology Use Guidelines. Staff and students are cautioned that even non-school division computer system use of social media that violates these Technology Use Guidelines, policy IIBEA, any School Board policies or procedures, the Code of Student Conduct, or creates a foreseeable risk of causing a substantial disruption to the work and discipline of the school, may result in disciplinary action. Students should only interact with staff

through social media sites created for educational purposes. Students should not engage staff through personal social media sites or accounts.

Social media in the classroom shall be used with students under the age of 13 years only where allowed by law (e.g., falls within the parameters of COPPA, CIPA, and PPRA) or when Winchester Public Schools has approved usage division-wide (e.g., the Winchester Public Schools Google Domain, a private WPS learning management tool) and with parental permission.

Staff may establish one or more social media accounts or accounts on educational websites solely for educational purposes. Staff must notify the building principal of their intent to establish such accounts and the building principal must approve and monitor each account. These accounts shall not be used for personal communications and are to be separate from staff members' personal social media accounts. Any such site shall have a clear statement of purpose and outcomes for the use of the account, and a code of conduct for all participants. The staff member establishing the account shall apply appropriate security and privacy settings, be responsible for the account's content, diligently monitor the account for inappropriate content, and post only information related to the account's purpose that is appropriate for viewing by students, parents and the community at large. Students should not be required to create a login in order to access or view the information. When appropriate, links to these accounts shall be posted on the school's webpage, as outlined in Policy CJA-Website Development and Management. Staff members are expected to read and understand all terms of service and privacy policies associated with the social media and educational site accounts they intend to use for instructional purposes.

Staff members are expected to be role models. Material posted on staff members' personal websites, accounts, and social media websites must model the behavior that staff members are expected to exhibit, as a role model, both on and off campus and school related activities. Inappropriate content, including without limitation, material that compromises a staff/student professional relationship or boundaries, messages and pictures that diminish a staff member's professionalism, discredits his/her capacity to maintain the respect of students and parents, or that impairs the ability of that staff member to serve as a role model for students, is prohibited. WPS expects the following in regards to personal electronic communications, use of social media, and other online communications.

WPS prohibits any students and staff members from establishing an online social media relationship through their personal social media websites. Interaction between staff and students on any social media websites must be for educational purposes only.

Staff and students shall not use Internet resources that require the establishment of a student account or login that is not administrated or monitored by WPS.

Google Domain. Winchester Public Schools has established and manages an instance of G Suite for Education, a set of productivity tools for classroom collaboration provided by Google, and utilizes additional services with the G Suite for Education platform as deemed appropriate and that support educational purposes at Winchester Public Schools.

Student Supervisory Guidelines. Teachers will provide students with a sequential, structured approach to gaining the skills that will allow them to become independent, responsible users of the

computer network or Internet. In all classes, teachers will make a reasonable effort to ensure that students are directed to sites with age and topic appropriate materials and resources.

Filtering Process. Winchester Public Schools recognizes that users may encounter materials that could be viewed as inappropriate and non-educational. Therefore, provisions have been made to direct and monitor student and staff use through the use of filtering software. The Technology Department manages the filtering software and School Division Administrators provide input regarding which categories of Internet sites as delineated within the software are to be blocked based to remain in compliance with the Children's Internet Protection Act (CIPA) and the Code of Virginia. Requests to block or unblock additional categories or specific sites are made by the requesting staff member through the Technology help desk ticket system. It continues to be the responsibility of the individual user not to initiate access to inappropriate material. If such material is encountered, the user is expected to exit immediately and notify the building administrators or Technology Department or the teacher of the inappropriate material and how it was accessed.

Use of Personal Devices. Students and Staff who utilize their personally owned devices at Winchester Public Schools facilities and/or on Winchester Public Schools' Computer System do so with the understanding that:

- They are held responsible for all aspects of these Technology Use Guidelines and all School Board policies, including but not limited to Policy IIBEA Acceptable Computer System Use, as they apply to devices utilized on Winchester Public Schools property and/or Winchester Public Schools' internal or external network.
- They utilize personally owned devices with the understanding they do so at their own risk. The school division is not liable for any theft, breakage, or damage to any personal device regardless of how that damage occurs (student discipline issues, drops, theft from locker rooms or hallways, power surges, and more)
- All Virginia Department of Education testing and school division course specific testing will be done on a school issued device so that the required secured browser is utilized according to testing standards.
- Users of personally owned devices do not have a right of privacy when connecting personally owned devices to WPS electronic media and networks.

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.

Areas of Responsibility. Staff and students must comply with, and are responsible for monitoring, enforcing, and reporting infractions of these Technology Use Guidelines as follows:

- Central office leadership (i.e., department supervisors, coordinators, directors, etc.) and building principals, assistant principals and other school-based administrators shall be responsible for ensuring that this Policy is followed. They shall also implement an internet safety program into

the division's curriculum in accordance with Virginia Department of Education guidelines and requirements.

- Principals or their designee will serve as the building-level coordinator for the Computer System and will support the building-level activities and Computer System, ensure that staff receives training pursuant to these guidelines and policy IIBEA, maintain student permission data, ensure that students receive training pursuant to these guidelines and policy IIBEA, and be responsible for implementing and interpreting these guidelines at the building level.
- Teachers shall be responsible for guiding and monitoring student use of the Computer System. Teachers shall also integrate safety instruction as designed and approved by the division into classroom curriculum.
- Students shall be responsible for adhering to these guidelines and policy IIBEA and using the Computer System for assignments directly related to the curriculum in a respectful and responsible manner. Students shall report any violations to these guidelines or policy IIBEA to a teacher or building administrator.
- Parents/Guardians are strongly advised to review these guidelines and policy IIBEA, ask questions if there are any regulations that they do not understand, work with their student(s) to ensure they understand these guidelines and policy IIBEA, and monitor their student(s) activities on the internet.

Technology Purchases. No equipment, software, or systems that connect to the Winchester Public Schools' network in any way or require Winchester Public Schools' computer resources of any kind shall be purchased without first consulting with the Director of Technology. The Director of Technology will be made aware of any such plan to purchase such technology during the initial evaluation of the product. The Director of Technology will advise on the compatibility and integration of the equipment, software, or system with the division's network and existing systems, and what additional resources will be required to support the product. It will not be the responsibility of the Technology Department to provide support for projects not in compliance with these guidelines without direction from the Superintendent or the School Board.