File: IIBEA

ACCEPTABLE COMPUTER SYSTEM USE

I. Purpose

The School Board supports the use of technology for purposes of educational research, communication, and instruction, and to provide access to unique resources and opportunities for collaborative work. In furtherance of its approved curriculum, the School Board provides a Computer System, which includes the Internet, the use of which must be consistent with this Policy, the educational objectives and work climate of Winchester Public Schools ("WPS" or the "Division") and other School Board policies, regulations, and directives.

The term Computer System includes, but is not limited to, hardware, software, data, communication lines and devices, display devices, printers, CD/DVD and other media devices, flash drives, servers, mainframe and personal computers, tablets, laptops, cellular and network phones, including smart phones, the Internet and all other electronic services and internal or external networks (the "Computer System"). All use of the Computer System must be for educational purposes or legitimate school business. The Computer System is not a public forum and is not intended to be a forum; its purpose is to advance the Division's communications, curriculum, and work. This Policy applies to all users of the Computer System. By using or accessing the Computer System, the user agrees to abide by this Policy.

Winchester Public Schools has established and manages an instance of G Suite for Education, a set of free 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 education purposes at Winchester Public Schools.

Use of the Computer System is a privilege, not a right, and can be withdrawn by the Division at any time, with or without prior notice. Any communication or material generated using the Computer System, including without limitation electronic mail, social media posts, instant or text messages, and other files, may be monitored, read, and/or archived by school officials without prior notice, reason, or permission, even if the communication or material was deleted from a user's account.

II. In General

A. The Computer System shall be used as follows:

1. The Computer System must be used for either an educational purpose or for legitimate school business. The term "educational purpose" includes, without limitation, use of the Computer System for class assignments; instruction, including the development and preparation of lessons and assignments; professional or career development; and otherwise in furtherance of the School Board's vision, mission, approved curriculum and other educational objectives.

2. The Computer System may not be used for commercial purposes. The term "commercial purposes" includes, without limitation, use of the Computer System

for the purpose of promoting or soliciting the sale of an item or the promotion or solicitation of a service that does not have an educational purpose or is not for legitimate school business; purchasing personal, family, or household items; to obtain a monetary or personal gain; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-profit. No staff member shall knowingly provide names, e-mail addresses, or other personal information to outside parties whose intent is to communicate with staff, students and/or their families for non-school purposes.

3. The Computer System may not be used for political lobbying or campaigning. This activity includes, without limitation, sending e-mails or making web postings or advertisements that advocate support for a particular political position or candidate; however, nothing in this Policy shall be construed to limit staff and students from using the Computer System to communicate with their elected representatives and to express their opinion on political issues for educational purposes.

B. The following definitions apply to this Policy:

1. The term "staff" or "staff member" is defined to include all School Board employees, including without limitation all administrators, counselors, teachers, coaches, employees of virtual school programs (to include but not be limited to distance learning, on line programs) and vendors providing instructional services to students, as well as all student teachers, interns and practicum students, volunteers and community members.

2. The term "immediately" is defined as reporting a situation that may constitute a violation of this Policy within twenty-four hours of the first suspicion of the violation.

III. Areas of Responsibility

Staff and students must comply with, and are responsible for monitoring, enforcing, and reporting infractions of this Policy as follows:

A. Central office managers (i.e., department supervisors and directors) and building principals and other school-based administrators shall be responsible for ensuring that this Policy is followed.

B. The Director of Technology will serve as the coordinator to oversee the Computer System and will work with other local, regional, or state organizations as necessary. All purchases of hardware, software, on-line resources, and other services must be evaluated and approved beforehand by the Director of Technology or designee.

C. The building principal or 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 this Policy, maintain student permission data, ensure that students receive training pursuant to this Policy, and be responsible for implementing and interpreting this Policy at the building level.

D. Teachers shall be responsible for guiding and monitoring student use of the Computer System.

E. Students shall be responsible for adhering to this Policy and using the Computer System for assignments directly related to the curriculum.

F. Parents and guardians shall be responsible for ensuring that their child(ren) adhere to this Policy and use the Computer System for curriculum related assignments.

IV. Internet Safety

A. Content Filtering. Pursuant to the federal Children's Internet Protection Act, 47 U.S.C. § 254, and Va. Code § 22.1-70.2, the Division shall select and implement a technology protection measure to filter or block Internet access, for both adult and minor users, through the Computer System, to material unrelated to the Division's educational vision, mission, and approved curriculum, and to:

1. Pornography, including child pornography, as defined by 18 U.S.C. § 2256 and Va. Code § 18.2-374.1:1;

2. Profane and obscene material, as defined by 18 U.S.C. § 1460 and Va. Code § 18.2-372; and

3. Material that the 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.

The technology protection measure will be enforced during any and all use of the Computer System as required by law. The current technology protection measures include without limitation managed networks, firewalls, Internet filters, virus controls, and monitoring devices. Despite its best efforts, it may not be possible for the Division to restrict access to all prohibited materials. User activity and the operation of filtering protection measures will therefore be monitored to ensure compliance with federal and state law, this Policy, and other School Board policies, regulations, and directives.

B. Student Training. Pursuant to Va. Code § 22.1-70.2, WPS will provide Internet safety training to all students. Internet safety instruction is integrated into the K-12 curriculum. Principals will review this Policy and other applicable School Board policies, regulations, and directives with staff and students annually.

C. Student and Staff Training. WPS will also provide students and staff training designed to educate about appropriate online behavior, including without limitation, appropriate conduct when using email, social media, blogs, and chat rooms, as well as cyber bullying awareness and response.

V. Access to the Computer System

A. Staff and students will have access to the Internet through selected computers and other electronic devices. Student use may be limited upon parental or guardian notification. Parents and guardians may request alternative activities for their child(ren) that do not require Internet access by notifying the building principal in writing or completing the Parent Permission Form for Student Involvement issued with the Student Handbook. Parents and guardians may also request to view the content of their child's user file.

B. Staff and students are permitted to use personal electronic devices, such as smart phones tablets, and laptops, provided that such use is consistent with this Policy and as set forth in Policy JFI- Student Use of Personally Owned Electronic Devices.

VI. Limitation of Liability. The School Board makes no warranties of any kind, neither express nor implied, regarding the Computer System. The School Board will not be responsible for any damages users suffer, including, but not limited to:

A. Loss of data resulting from delays or interruptions in service;

B. Accuracy, nature, or quality of information stored on the Computer System;

C. Accuracy, nature, or quality of information gathered through the Computer System;

D. Damage to personal property used to access the Computer System; or

E. Unauthorized financial obligations resulting from use of the Computer System.

VII. Unacceptable Uses of the Computer System

A. WPS shall cooperate fully with local, state, and/or federal officials in any investigation concerning or relating to any alleged illegal activities conducted through the Computer System.

B. Students who violate the provisions of this Policy, applicable state and federal law, applicable School Board policies, regulations, and directives, and/or applicable building-level rules shall be subject to disciplinary action in accordance with Policy JFC Student Conduct..

C. School Board employees who violate the provisions of this Policy, applicable state and federal law, applicable School Board policies, regulations, and directives, and/or applicable building-level rules shall be subject to disciplinary action in accordance with the School Board personnel policies.

D. Non-employees violating this Policy shall have their access privileges immediately suspended.

VIII. Computer System Monitoring and Related Searches

A. Users have no right of privacy and should have no expectation of privacy in materials sent, received, or stored on the Computer System. The Division reserves the right to monitor and review all usage of the Computer System at any time, for any reason, with or without prior notice or permission.

B. Routine maintenance and monitoring of the Computer System may lead to the discovery that the user has or is violating this Policy or other School Board policies, regulations, and directives.

C. A search of a user's account shall be conducted if there is individual reasonable suspicion that a user has violated the law or School Board policies, regulations, or directives. The nature of the search/investigation will be reasonable and appropriate to the nature of the alleged misconduct.

D. User files may be subject to protection and disclosure requirements set forth in the Family Educational Rights and Privacy Act (FERPA), Individuals with Disabilities Education Act (IDEA), the Freedom of Information Act (FOIA), and other federal and state laws.

E. Users must provide their password upon request to technology staff for use in diagnosing and repairing Computer System problems and in providing routine maintenance and monitoring of the Computer System. In the event an account or password is known or suspected to have been lost, stolen, or disclosed, the user shall immediately report the incident to technology staff and new passwords will be created.

IX. Software and Hardware. Only school or Division licensed software approved by the Director of Technology may be installed on the Computer System. No school-licensed software may be copied for use on other school's Computer System unless this right is specifically granted in the school's license agreement. Software may only be installed by technology staff members. All licensing and registration materials shall be furnished to the building Technology Resource Teacher, who is responsible for maintaining licensing records on a building level. The Director of Technology will maintain records on Division licensed software.

X. Selection of Material. When using the Internet for class activities, staff shall select material that is appropriate in light of the age of the students, relevant to the course objectives,

and consistent with the Division's approved curriculum and educational mission, vision and objectives. Staff shall preview the materials and sites they require or recommend students to access in order to determine the appropriateness of the material contained on or accessed through the site. Staff shall provide guidelines and lists of resources to assist students in channeling their research activities effectively and properly. Staff shall assist their students in developing the skills to evaluate the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

XI. Acceptable and Unacceptable Use

A. Acceptable Use. Use of the Computer System shall be consistent with the educational vision and mission, approved curriculum, and work of the Division, as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. Staff are to utilize the Computer system for educational purposes, legitimate school business, and performance of job duties. Incidental personal use of the Computer System is permitted as long as such use does not interfere with the staff member's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications not occurring during instructional time and is not otherwise prohibited by this Policy.

B. Unacceptable Use. The following is a non-exhaustive list of examples of unacceptable uses of the Computer System:

1. Engaging in Illegal and other Unacceptable Activities. Users shall not use the Computer System to:

    a. "Hack into" or otherwise access data not intended for the user, including, without limitation, logging into another user's account or otherwise obtaining another user's files or administrative data.

    b. Make deliberate attempts to disrupt the Computer System or destroy data by spreading computer viruses or by any other means.

    c. Send, receive, view or download illegal material, or engage in any other illegal act, including, without limitation, arranging for the sale or purchase of illegal drugs, alcohol or tobacco, engaging in criminal gang activity, or threatening the safety of another individual.

    d. Access, upload, download, create, or distribute profane, pornographic, obscene, sexually explicit, or other illegal material.

    e. Transmit profane, obscene, abusive, sexually explicit, or threatening language that could be characterized as bullying, harassing, prejudicial or discriminatory attacks, or is otherwise damaging to one's reputation.

f. Vandalize, damage, or disable the property of another individual or organization, including destroying data by creating or spreading viruses or by other means.

g. Violate any other local, state, or federal law.

h. Delete, erase or otherwise conceal any information stored on the Computer System that violates this Policy or at any time after being advised by an administrator or supervisor to preserve any materials stored on the Computer System.

2. Jeopardizing System Security

a. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from accessing their accounts. Under no conditions should a user provide password information to another person except as provided in this Policy.

b. Users shall not alter system or network settings, circumvent the menu, password, or Internet filtering software installed on the Computer System, or change configurations (hardware and software), except under the direct supervision of technology staff.

c. Users shall immediately notify the Director of Technology if they have identified a possible security problem.

d. Users shall insure that the latest antivirus/antimalware software is installed and functioning on their personal electronic device when it is connected to the Computer System.

3. Using Inappropriate Language

a. Restrictions against inappropriate language apply to messages and posts made on or through the Computer System, including without limitation public messages, private messages, email, and material posted on Division, school, and extracurricular organization webpages or related social media accounts.

b. Users shall not use the Computer System to convey or otherwise disseminate obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

c. Users shall not use the Computer System to post or email information that, if acted upon, could cause damage or a danger of disruption.

d. Users shall not use the Computer System to knowingly or recklessly post false or defamatory information about a person or organization.

Failure to Respect Privacy

a. Users shall not use the Computer System to publicize a message that was sent to them privately without permission of the person who sent the message.

b. Users shall not use the Computer System to post or email private information about themselves.

c. Users shall not use the Computer System to disclose, use, or disseminate photographs and/or personal information regarding other people. Personal information is defined to include information such as a person's home address, telephone number, social security number, bank or credit card account number, log-in information or password.

4. Failure to Respect Resource Limits

a. Staff shall not download large files on the Computer System unless absolutely necessary. If necessary, large files shall be downloaded only at a time when the Computer System is not being heavily used. All files downloaded shall be for educational purposes or legitimate school business. Students shall not download any files.

b. Users shall not use the Computer System to post or email chain letters or to engage in "spamming." For purposes of this Policy, spamming is defined to include sending an unnecessary message, unrelated to educational purposes or legitimate school business, to a large number of people.

c. Users may not use the Computer System to subscribe to discussion groups or e-mail lists, unless such groups or lists are relevant to an educational purpose or legitimate school business, including a specific assignment or for instructional purposes.

d. Users shall not abuse or monopolize the Computer System for non-educational use.

5. Plagiarism and Copyright Infringement

a. Users shall not plagiarize works found on the Computer System. Plagiarism is taking the ideas or writings of others and presenting such ideas or writings as if they were original to the user.

b. Users shall respect the rights of copyright owners. The School Board Policy EGAA Reproduction of Copyright Materials applies to copyrighted materials accessed through the Computer System, as well as traditionally published materials. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, users should request permission from the copyright owner.

7. Student Acceptable Use of Email and Other Electronic Communication. Student access to direct electronic communications, including e-mail, shall be made via a special account assigned to each student and used under staff supervision, provided that the following restrictions are met:

   a. Students shall not use the Computer System to post or e-mail personal or sensitive information about themselves or other people. This includes information such as the student's or another person's home address, telephone number, student ID number, bank or credit card account numbers, social security numbers, login information and passwords.

   b. Students shall not use the Computer System to meet with someone they have met online without their parent's or guardian's prior approval and participation.

   c. Students shall promptly disclose to their teacher or other school staff any message they receive that is inappropriate or makes them feel uncomfortable.

8. Staff Acceptable Use of Email and Other Electronic Communication

   a. **In General**. The Computer System provides opportunities for increased communication and collaboration for both students and staff. As students and staff are connected to the global community, their use of new tools and systems brings new responsibilities. Any electronic or online communications by staff with other staff, students and parents must be transparent, accessible to supervisors and parents, and professional in content and tone.

      Electronic communications should not replace in person and telephone communication, which are better modes of communication for conveying meaning and context and should be used whenever possible.

      Staff using electronic and online communication shall adhere to the following guidelines:

i. Any staff member who has a reason to suspect that inappropriate communication is occurring between a staff member and student or among staff members shall report the matter immediately to their principal.

ii. Staff members who correspond with students or parents via email must use only the Division's email system to receive or send email. Staff correspondence with students is strictly limited to school related content.

iii. Staff members who correspond with other staff members about school related business must use only the Division's email system to receive or send email.

iv. Staff should not include detailed student information in any email or document attached to an email. Staff shall not use or attach a document that reveals a social security number, biometric record, or student identification number that could be used directly or indirectly to gain access to education records. When referencing students, the email shall be limited to basic factual information and exchanged only between parties who have a legitimate educational interest in the information and in the student that is the subject of the correspondence.

v. Electronic resources must never be used to discuss contentious, sensitive, emotional or highly confidential issues. These issues should be discussed in person or by phone. Emails should be short and directional in nature and only include objective factual information. Examples of such factual information are set forth in Section 8(B) below.

vi. Staff members are responsible for all email sent from their account, and should take care to protect access to their account by keeping their password secret and by logging off when not using their account.

vii. Electronic communication should be consistent with professional practices for other correspondence. This includes grammar, format and salutation.

b. **Acceptable uses of staff to parent email or other electronic communication.** Examples of this acceptable use includes providing general information about class activities such as curriculum, homework, tests, special events and school announcements; making arrangements for meeting/telephone call regarding a student issue, including a general description of the issue; and following-up on an issue that has previously been

discussed. Any discussion related to other students or staff members is not appropriate.

c. **Acceptable uses of staff to student email or other electronic communication.** Examples of this acceptable use includes discussions specifically related to class activities, such as curriculum, homework, tests, special events, and school announcements. There should be no discussion related to other students, discussion about the personal life of staff members or students, or sensitive information regarding the student's performance.

d. **Establishment of social media accounts or accounts on educational sites for instructional purposes**. 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.

e. **Personal social media accounts.** 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:

    i. 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 a social media websites must be for educational purposes only, as set forth in section XI(B)(8)(d) above.

ii. 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.

iii. Students appearing in individual or group photographs shall not be individually identified.

iv. Staff shall not post comments about students.

XII. Non-Computer System Use. The School Board has no legal responsibility to regulate or review Internet messages, statements, postings, or acts either made off-campus or not made on, through, or in connection with the Computer System. The Division reserves the right to discipline students and staff for actions taken off-campus or independently of the Computer System, which would violate this Policy or other applicable School Board policies, regulations or directives if occurring on-campus or on, through, or in connection with the Computer System, if such actions adversely affect the safety, well-being, or performance of students while in school, on school buses, at school activities or school sponsored events, or coming to and from school; if such actions threaten violence against another student or staff member; if such actions violate local, state or federal law; or if such actions disrupt the learning environment, administration, or orderly conduct of the school.

XIII. Remote Access to the Computer System. All provisions of this policy apply when accessing the Computer System remotely or on-site.

XIV. Acceptable Computer System Use Agreement. Each staff member, student and parent/guardian of each student shall sign the Acceptable Computer System Use Agreement before using the Computer System. The failure of any staff member or student to follow the terms of the Agreement or this Policy may result in the loss of Computer System privileges, disciplinary action, and/or appropriate legal action.

X. Review. The School Board will review and amend, if necessary, this Policy every two years.

Adopted:
May 19, 2003, Revised September 6, 2005, September 5, 2006, October 1, 2007, August 16, 2010, March 14, 2011, January 6, 2014 subject to review & re-approval by December 31, 2014, June 12, 2017

Legal Refs: 18 U.S.C. sections 1460, 2256
47 U.S.C. section 254

Va. Const. art. VIII § 7

Code of Virginia, 1950, as amended, sections 18.2-372, 18.2-374.1:1, 18.2-390, 22.1-70.2, 22.1-78, 22.1-79

Guidelines and Resources for Internet Safety in Schools, Virginia Department of Education (Second Edition October 2007)

Guidelines for the Prevention of Sexual Misconduct and Abuse in Virginia Public Schools (Approved by the Board of Education March 24, 2011)