Policy Code: 6161 Acceptable Use of Technology

~~June 2025~~ April 2026

I. **PURPOSE**. To transform the educational experience and foster vital connections, the Winston-Salem/Forsyth County Board of Education ("the Board") provides students and staff access to essential digital tools, network infrastructure, and online resources. These technologies empower users to personalize learning, collaborate effectively locally and globally, access diverse and current information instantly, create innovative content, engage critically with worldwide events and perspectives, and develop skills as responsible digital citizens in our interconnected world.
The Board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal and responsible use. Accordingly, the Board establishes this policy to govern student and staff use of school district digital tools. This policy also applies to any non-students who are expressly authorized by the school district to use electronic information resources, including, but not limited to, Board of Education members, contractors, consultants, and temporary workers. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

II. **DEFINITIONS**

A. **Technology Resources** – digital tools, systems, and infrastructure provided or made available by the Board for educational and administrative purposes. This includes (but is not limited to) physical and wireless network and internet access including the Winston-Salem Forsyth County Schools (WS/FCS) guest wireless network, staff and student account credentials, email, online software applications and digital content, and hardware such as laptops, chromebooks, tablets, smartphones, printers, scanners, projectors, interactive panels.

B. **User -** any individual person of any age including a student, employee, contractor, volunteer, or community member that accesses district provided technology resources or network.

III. **SCOPE OF USERS**

By accessing any of the district's networks or using any district provided device, all students, employees, contractors, volunteers, and community members are automatically included and required to comply with this Acceptable Use policy. This means that upon the first instance of accessing district provided technology resources, the user agrees with the terms of this Acceptable Use policy.

IV. **EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES**.

The use of district technological resources is a privilege, not a right. Individual users of the school district's technological resources are expected to use such resources in a manner that is ethical, respectful, academically honest and supportive of student learning.

If a student or employee violates a WS/FCS policy or administrative regulation in the course of using district technological resources, that person may be disciplined according to WS/FCS rules/procedures and/or prosecuted in accordance with state and/or federal law. In particular, students and employees should be aware of the following policies and regulations while using district technological resources:

1. AR 1111**: Use of School Mail, Cellular Telephones, Fax and E-mail**
2. **Policy** 1170**: Civility Policy**
3. **Policy** 1311**: Political Activities in Schools**
4. **Policy** 1324**: Soliciting Funds From and By Students By Charitable Organizations**
5. **Policy** 1325**: Advertisement and Promotional Activities**
6. **Policy** 4116.10**: Standards of Professional Conduct**
7. **Policy** 5125**: Privacy of Student Records**
8. **Policy** 5131**: Student Behavior**
9. AR 5131**: Code of Student Conduct**
10. **Policy** 5131.1**: Discrimination, Harassment and Bullying**
11. **Policy** 6161.1**: Website Policy**
12. **Policy** 6161.2**: Internet Safety**
13. **Policy** 6161.3**: Selection Standards for Supplementary Textbooks and Use of Other Instructional Materials**

V. **RULES OF USE OF SCHOOL TECHNOLOGIAL RESOURCES**.

The following rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

1. School district technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Because some incidental and occasional personal use by employees is inevitable, the Board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school district business and is not otherwise prohibited by Board policy or procedure.
2. School district technological resources are installed and maintained by members of the Technology Services Department. Users shall not attempt to perform any installation or maintenance without the permission of the Technology Department.
3. Under no circumstance may software purchased by the school district be copied for personal use.
4. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Student Code of Conduct.
5. School employees must not disclose on school district websites or web pages or elsewhere on the internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or **Policy** 5125**: Privacy of Student Records.**
6. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading,

storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

7. The use of virtual private networks (VPN), proxy websites, or any application or service designed to hide activity, mask identity, or bypass network security and safety protocols is strictly prohibited.
8. Users may not install or use any WS/FCS provided device, network, or other technology resource that facilitates the downloading, uploading, or distribution of copyrighted content without proper authorization.
9. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Any user caught inflicting intentional or negligent damage to any technological resource will be subject to financial charges for repair, replacement, or loss of data or access to systems.
11. Users may not create, install, or run any games, software, or network-based programs (such as chat apps or file-sharing tools) on district computers, devices, or networks without prior approval from the Technology Director or an authorized staff member. This includes any programs not provided or approved by the school for educational use.
12. Users may not attempt to gain unauthorized access to systems, networks, or accounts (commonly known as “hacking”), or engage in any activities intended to disrupt or compromise the security or functionality of school technology.
13. Users are prohibited from using another individual’s userID or password for any technological resource.
14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner’s express prior permission.
15. Users shall not use userID’s or passwords for any technology resource or system for an unauthorized or improper purpose.
16. If a user discovers a security issue on any school device, system, or network, they must report it immediately to a teacher, technology staff member, or system administrator. Users should not attempt to test, share, or demonstrate the issue to other users. Anyone found to be intentionally compromising system security may lose access to district technology resources.
17. Teachers and school administrators shall make reasonable efforts to supervise students’ use of technological resources during instructional time to ensure that such use is appropriate, educationally purposeful, and aligned with district policies. This includes guiding students in the proper care, handling, and responsible use of devices, and addressing any misuse or damage promptly.
18. Users may connect personal devices such as laptops, iPads, tablets and smartphones to the WS/FCS guest Wi-Fi network. Personal technological devices will not be supported by WS/FCS technical staff.
19. Only district-provided or district-approved cloud storage and collaboration platforms may be used for storing or sharing district-related information, especially sensitive or confidential data. When accessing these approved services using personal devices or third-party applications,

users remain responsible for safeguarding data privacy and adhering to all relevant district policies and data protection laws. Unauthorized platforms or services should not be used for district activities.

VI. **RESTRICTED MATERIAL ON THE INTERNET**. The digital landscape, encompassing the internet and electronic communication, is dynamic and constantly evolving. This fluidity provides students with access to a vast array of information and perspectives from numerous and rapidly changing sources. However, it also means that students may encounter content that is potentially inappropriate or harmful. While our school district is committed to providing a safe and productive online environment, it's important to acknowledge that the ever-changing nature of the internet makes it impossible to guarantee the complete prevention of exposure to all potentially harmful material. Nevertheless, the district has implemented robust, multi-layered safeguards, including a hosted and filtered internet environment, designed to minimize student access to content that is obscene, pornographic, or otherwise harmful to minors, such as material depicting violence, nudity, or graphic language. These measures are in full compliance with the Children's Internet Protection Act (CIPA). To maintain the integrity of our safety protocols, technology protection measures will only be temporarily adjusted or disabled for authorized employees when essential for specific job responsibilities and with the explicit approval of Chief Technology Officer or their designated representative.

VII. GENERATIVE ARTIFICIAL INTELLIGENCE (AI).

The Board recognizes that generative artificial intelligence (AI) tools support teaching, learning, and operational efficiency when used appropriately. All use of AI must align with district expectations for ethical, responsible, and academically honest use of technology as outlined in this Acceptable Use of Technology Policy, including compliance with data privacy, security, and intellectual property laws and policies. Users are responsible for the accuracy, appropriateness, and integrity of any content created or supported by AI tools. The use of AI to misrepresent work, violate privacy, or create deceptive or harmful content is prohibited. Additional guidance, expectations, and approved practices for AI use are outlined in the district's Generative AI Guidelines

~~VII.~~VIII. **PARENTAL CONSENT**

Aligned with the school Board's vision for leveraging technology in education, students may be required to utilize accounts on select third-party platforms for specific, curriculum-integrated projects. These activities are intentionally designed to cultivate effective and responsible online communication skills and support other key learning objectives. While we are committed to providing these enriching digital experiences, we also respect parental preferences.

For certain limited third-party services, such as YouTube, which may be used to access educational content, parents/guardians who have concerns or wish to opt their student out of their use can do so by contacting their student's school administration to understand the available procedures.

Where the creation and management of third-party accounts necessitates explicit parental consent under applicable regulations, the school will proactively obtain that permission.

VIII. **PRIVACY**. In general, no right of privacy exists in the use of school district technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the Superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with Board policy and applicable laws and regulations. Under certain circumstances, the Board may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the Board, as a response to a public records request or as evidence of illegal activity in a criminal investigation. Certain types of communications and documents may be protected by privacy laws such as student records, personnel records, and exceptional children's records.

IX. **SECURITY AND CARE OF PROPERTY**. Security on any computer system is a high priority, especially when the system involves many users. Employees must enable passcode or password-protected lock screens on district issued tablets, smartphones, laptops, desktop computers, and other such devices. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the district network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access. Users are to follow all instructions regarding maintenance or care of school technological equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for such equipment.

X. **DISCLAIMER**. The Board makes no warranties of any kind, whether express or implied, for the service it is providing. The Board will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors or omissions. Use of any information obtained via the internet is at the user's own risk. The school district specifically disclaims any responsibility for the accuracy or quality of information obtained through its internet services.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e)

Adopted: June, 1996

Adopted: July 1, 1995

Revised: May, 2000; September 2008; March 2014; June 2025; April 2026

Winston-Salem/Forsyth County Schools