

Book	BOARD POLICES
Section	7000 BP - Property
Title	STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	7540.04 BP
Status	Active
Adopted	September 10, 2024

## STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

### Reference:

P.L. 106-554, Children's Internet Protection Act of 2000  
P.L. 110-385, Title II, Protecting Children in the 21st Century Act  
18 USC 1460  
18 USC 2246  
18 USC 2256  
20 USC 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)  
47 USC 254(h), (1), Communications Act of 1934, as amended (2003)  
47 C.F.R. 54.520

Technology directly affects the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt their means and methods of instruction and the way they approach student learning to incorporate the latest technologies. The Board of Directors provides Academy Information & Technology Resources (as defined by Bylaw 0100) (collectively, "Academy Information & Technology Resources") to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The Academy's computer network and Internet system does not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its stated educational purpose.

The Board regulates the use of Academy Information & Technology Resources by principles consistent with applicable local, State, and Federal laws and the Academy's educational mission. This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staff's use of the Academy's Information & Technology Resources and staff's personal communication devices when they are connected to Academy Information & Technology Resources, including online educational services/apps, regardless of whether such use takes place on or off academy property (see Policy 7530.02).

Staff members are prohibited from using Academy Information & Technology Resources to engage in illegal conduct (e.g., libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, etc.) or conduct that violates this Policy and its related administrative guidelines (e.g., making personal attacks and injurious comments, invading a person's privacy, etc.). Nothing herein, however, shall infringe on a staff member's First Amendment rights. Because Academy Information & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Staff members have no right or expectation to privacy when using Academy's Information & Technology Resources (including, but not limited to, privacy in the content of their personal files, messages/e-mails, and records of their online activity).

Staff are expected to use Academy Information & Technology Resources to promote educational excellence in our academy by providing students with the opportunity to develop the resource-sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services/apps will be guided by Board Policy 2521 – Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that brings incredible education and information resources to our students. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, Academy Information & Technology Resources provide students and staff with the opportunity to communicate with people throughout the world. Access to such an incredible quantity and diversity of information and resources brings with it, however, certain unique challenges and responsibilities.

While the Board uses various technologies to limit the use of Academy Information & Technology Resources to only use/access online services/apps and resources that have been pre-approved for the purpose of instruction, study, and research related to the curriculum, it is impossible to prevent users from accessing and/or coming in contact with online content that has not been pre-approved for use by students of certain ages. It is no longer possible for educators and community members to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted procedures and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them) when significant portions of students' education take place online or through the use of online educational services/apps.

Pursuant to Federal law, the Board has implemented technology protection measures, that, protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or Educational Service Provider, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. However, the Board is cognizant of the fact that such software and/or hardware is not perfect and relies on Staff members to self-police (and immediately cease viewing) online activity that would otherwise be in conflict with these policies and to immediately report such to the Educational Service Provider. The technology protection measures may not be disabled at any time that students may be using the Academy Information & Technology Resources, if such disabling will cease to protect against access to materials that are prohibited under CIPA. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be disciplined, up to and including termination.

The Educational Service Provider or IT Department may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Educational Service Provider or IT Department may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

The Educational Service Provider, is directed to prepare procedures which address students' safety and security while using e-mail, chat rooms and other forms of direct electronic communication, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by minors online. Staff members are reminded that personally identifiable student information is confidential and may not be disclosed without prior written parental permission.

The Educational Service Provider is responsible for providing training so that staff under their supervision are knowledgeable about this policy and its accompanying guidelines.

The Board directs the Educational Service Provider to initiate professional development programs in accordance with the provisions of law and this policy. Training shall include:

- A. the safety and security of students while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
- B. the inherent danger of students disclosing personally identifiable information online;
- C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students or staff online; and
- D. unauthorized disclosure, use, and dissemination of personally-identifiable information regarding minors.

Staff members shall provide guidance and instruction to their students regarding the appropriate use of Academy Information & Technology Resources and online safety and security as specified above. Additionally, such training shall include, but not be limited to, education concerning appropriate online behavior including interacting with others on social media, including in chat rooms, and cyberbullying awareness and response. Further, staff members shall monitor students' online activities while the students are at the academy.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

All staff members who use Academy Information & Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying procedures. (See Form 7540.04 F1)

In order to keep Academy Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, staff members are required to comply with all Academy-established cybersecurity procedures for which they have been trained. The Educational Service Provider is responsible for providing such training on a regular basis and measuring the effectiveness of the training.

Staff will be assigned an Academy-provided e-mail address that they are required to use for all academy-related electronic communications, including those to students, parents and other constituents, fellow staff members, and vendors or individuals seeking to do business with the Academy.

With prior approval from the Educational Service Provider or IT Department, staff may direct students who have been issued Academy-assigned e-mail accounts to use those accounts when signing up/registering for access to various online educational services/apps that the student will use for educational purposes under the teacher's supervision.

The Board expects all Academy personnel to be responsible for good behavior on when using Academy Information & Technology Resources – i.e., behavior comparable to that expected when in physical classrooms, academy buildings, and at academy-sponsored events. Because communications on the Internet are often public in nature, general rules for professional behavior and communication apply. The Board does not approve any use of Academy Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Staff member use of Academy Information & Technology to access or use social media is to be consistent with Policy 7544 and its accompanying procedure.

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the Academy's mission, undermine staff relationships, or cause a substantial disruption to the academy environment. This warning includes staff members' online conduct that occurs off academy property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

### **Use of Artificial Intelligence/Natural Language Processing Tools**

Staff are permitted to use Artificial Intelligence and Natural Language Processing (NLP) tools (collectively, "AI/NLP tools") to accomplish their job responsibilities so long as the use is ethical, responsible, and does not violate any provisions of this policy (e.g., it does not infringe on students' or staff members' privacy rights, violate their duty to maintain confidentiality related to personally identifiable information, etc.).

With respect to students, it is the Board's policy that they are required to rely on their own knowledge, skills, and resources when completing school work. In order to ensure the integrity of the educational process and to promote fair and equal opportunities for all students, except as outlined below, students are prohibited from using AI/NLP tools to complete school work. The use of AI/NLP tools without the express permission/consent of a teacher is considered to undermine the learning and problem-solving skills that are essential to a student's academic success and that the staff is tasked to develop in each student. Consequently, students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI/NLP tools, and they are expected to ask their teachers when they have questions and/or need assistance. A student's unauthorized use of AI/NLP tools is considered a form of plagiarism and any student found using such tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code of Conduct.

Notwithstanding the preceding, students are allowed to use AI/NLP tools in the academy setting if they receive prior permission/consent from their teacher, so long as they use the AI/NLP tools in an ethical and responsible manner. Teachers have the discretion to authorize students to use AI/NLP tools for the following uses:

- A. Research assistance: AI/NLP tools can be used to help students quickly and efficiently search for and find relevant information for their academy projects and assignments.
- B. Data Analysis: AI/NLP tools can be used to help students to analyze, understand, and interpret large amounts of data, such as text documents or social media posts. This can be particularly useful for research projects or data

analysis assignments – e.g., scientific experiments and marketing research.

- C. Language translation: AI/NLP tools can be used to translate texts or documents into different languages, which can be helpful for students who are learning a new language or for students who are studying texts written in a different language.
- D. Writing assistance: AI/NLP tools can provide grammar and spelling corrections, as well as suggest alternative word choices and sentence structure, to help students improve their writing skills.
- E. Accessibility: AI/NLP tools can be used to help students with disabilities access and understand written materials. For example, text-to-speech software can help students with specific learning disabilities or visual impairments to read texts and AI-powered translation tools can help students with hearing impairments to understand spoken language.

As outlined above, under appropriate circumstances, AI/NLP tools can be effectively used as a supplement to and not a replacement for traditional learning methods. Consequently, with prior teacher permission/consent, students can use AI/NLP tools to help them better understand and analyze information and/or access course materials. If a student has any questions about whether they are permitted to use AI/NLP tools for a specific class assignment, they should ask their teacher.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of Academy Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Educational Service Provider as responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff member use of Academy Information & Technology Resources.

In addition, Federal and State confidentiality laws forbid academies and Academy staff from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Academy personnel who violate State and Federal confidentiality and/or privacy laws related to the disclosure of student or staff personally identifiable information may be disciplined.

© National Charter School Institute