The Vanguard School

POLICY: Vanguard EHAA – Acceptable Technology Use Policy

POLICY ADOPTED: 4-15-26

1. Introduction

The Vanguard School (Vanguard) provides access to computers, network systems, internet services, and other electronic devices, collectively referred to as "technology resources," to support education, school-sponsored activities, and general school operations. This policy establishes rules governing the use of school-owned technology resources by students and staff. Use of Vanguard technology resources requires compliance with this policy and all other applicable school policies.

2. Rights and Expectations

Staff and students are expected to use technology in ways that reflect the school's mission and values. Any user who becomes aware of suspected misuse of technology resources shall report the matter to the IT Department or Assistant Principal.

To maintain a secure and functional technology environment, The Vanguard School retains the right to:

- Log and monitor network activity and account usage at any time, with or without notice.
- Restrict or revoke access to school technology resources.
- Restrict access to online destinations through filtering software or other technical controls.
- Determine whether specific conduct is in violation of this policy.

Users have no expectation of privacy when using school-owned devices, systems, or accounts. All materials accessed, transmitted, or stored through school technology systems may be reviewed by authorized personnel as necessary to maintain system functionality and security.

3. Acceptable Use

School technology resources are provided to support education, school-sponsored activities, and general school operations.

A. Staff

Nearly all staff rely on computer access on a daily basis to fulfill their job duties. Common examples of acceptable uses include:

- Online lesson planning or curriculum-related research
- Managing data in the student information system
- Accessing websites necessary to fulfill job duties
- Incidental personal use that does not interfere with job responsibilities.

B. Students

Students in all grades interact with technology to some degree on a daily basis, with the level of interaction increasing in Junior High and High School. Common examples of acceptable uses include:

- Taking online standardized tests
- Completing online assignments or project research
- Researching colleges and submitting college applications

C. Individual Educational Interests

Students may use school computers during study periods for individual educational interests only after completing assigned coursework due the next school day, or when assigned coursework cannot reasonably be completed at school. Classes scheduled to use computers take priority over individual student use. Students completing assigned coursework take priority over those using computers for individual educational interests.

Acceptable educational interests include, but are not limited to:

- Reading educational articles
- Practicing typing skills
- Practicing computer programing
- Photography editing
- Educational games

4. Prohibited Conduct

Vanguard shall take reasonable measures to ensure the safety and security of school information systems, users, and data. This relies, in part, on users avoiding the following prohibited activities while using school technology resources:

A. Academic Integrity Violations

(1) Students will not plagiarize content found on the internet or from other system users.
(2) Students will not submit work generated by artificial intelligence systems without authorization as outlined in Section 5.

B. Safety and Conduct Violations

(1) Students and staff will not post information intended to cause harm, danger, or substantial disruption.
(2) Students and staff will not engage in personal attacks or harass another person.
(3) Students and staff will not knowingly or recklessly post false or defamatory information.
(4) Students and staff will not use speech that is inappropriate in an educational setting or violates school rules.
(5) Students will not share personal contact information about themselves or other people.
    - Personal contact information includes your name, phone number, address, and email address.
(6) Students will not use Vanguard technology resources for social networking, third-party online chats, or high-bandwidth activities such as video streaming unless explicitly authorized by a staff member for a specific task.

C. System Integrity Violations

(1) Accessing or attempting to access another user's account (including sharing passwords)
(2) Downloading or installing software without authorization from the IT Department
(3) Attempting to bypass, disable, or modify security controls, including internet content filters
(4) Attempting to harm or destroy equipment, data, the network, or applications
(5) Modifying shared equipment such that it adversely impacts its functionality for others
(6) Introducing malware to school systems
(7) Disrupting network operations or interfering with the use of technology by others

D. Unauthorized Use

(1) Use of technology resources for non-school-related purposes, except as permitted by this policy
(2) Student use of personal technology devices (PTD) while at school except as permitted under Vanguard Policy JICJ
(3) Student connecting a personal technology device (PTD) to the network without explicit authorization
(4) Student playing online games, unless adhering to the guidelines in Section 3C
(5) Student using school computer without staff supervision
(6) Commercial activity, for-profit use, or political lobbying

5. Artificial Intelligence and Emerging Technologies

Large Language Models (LLMs) and other forms of artificial intelligence (AI) are increasingly available and capable. The Vanguard School recognizes both their potential utility and their danger to academic integrity and critical thinking.

A. Student Use

Students may use AI tools only as explicitly permitted by a teacher, in alignment with current learning objectives.

Examples of permitted use:

- Generating practice questions for study
- Exploring different ways to think about a difficult math concept
- Using an AI application as an opponent in a class debate to teach students how to support their positions against a well-equipped critic

Students may not submit AI-generated content, in whole or in part, as original work unless explicitly authorized by the teacher. Any submission of such content will be considered plagiarism/cheating and will result in the standard academic consequences.

B. Staff Use

All staff may use AI within the confines of pre-defined administrative and supervisory guidance, in support of their job duties. Staff shall not input confidential or personally identifiable student information into AI systems unless explicitly authorized by the Executive Director or his designee, and in compliance with applicable privacy laws and school policy.

Teachers may use AI systems as supportive tools for class preparation, instruction, assessment, or communication; however, teachers remain the content and instruction expert and are responsible for the accuracy and instructional integrity of all content used.

Examples of permitted use:

- Using an AI tool to support lesson planning
- Using an AI tool to assess student work for plagiarism
- Using AI to revise an e-mail for grammar and tone
- Demonstrating ethical use of AI in front of the class as it relates to the current lesson

To avoid perceptions of unfairness and model ethical behavior, teachers should disclose their uses of AI tools to their students and explain their reasoning and methods.

Future Developments

Given the rapidly evolving nature of AI, the Executive Director, or his designee, may develop further rules, guidelines, and procedures around the use of AI tools within the bounds of this policy.

6. Children's Internet Protection Act (CIPA)

It is the policy of The Vanguard School to comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]. As such, this policy satisfies the requirement to create an Internet Safety Policy mandating the following requirements:

- Technology protection measures that restrict access to inappropriate material on the internet that are obscene, are child pornography, or are harmful to minors
- Ensuring the safety and security of students and staff when using direct electronic communications
- Addressing unauthorized access, including "hacking," and other unlawful activities
- Addressing unauthorized disclosure, use, and dissemination of personal information regarding minors
- Monitoring the online activities of minors
- Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response

Additionally, CIPA requires that schools provide reasonable notice and hold at least one public hearing or meeting to address the required policy. Vanguard shall continue to comply with public notice and hearing requirements associated with CIPA.

Limitations

The Vanguard School shall make reasonable efforts to block inappropriate material on the internet as required by CIPA; however, Vanguard also recognizes that it is impossible to restrict access to all controversial, inaccurate, or inappropriate material on the internet. Vanguard does not have complete control over the effectiveness of filtering programs. Therefore, the school may not be held liable for inappropriate or controversial content accessed over the network provided reasonable efforts consistent with CIPA requirements were made.

7. Consequences for Violations

Suspected violations shall be reported to the IT Department. Consequences for student or staff violations of this policy shall be decided by school administrators on a case-by-case basis in accordance with applicable laws and other policies. Potential consequences include, but are not limited to:

- Supervised computer use
- Suspension of computer privileges
- Suspension of network privileges
- Suspension from school (*students*)
- Expulsion from school (*students*)
- Termination of employment (*staff*)
- Legal action

Initial adoption: 1-15-2019