The Vanguard School

POLICY: Vanguard EHAA – Acceptable Technology Use Policy

POLICY ADOPTED: 1-15-19

Introduction

The Vanguard School (Vanguard) provides information technology resources to students and staff solely for educational purposes. Student use of school computers, networks, and internet services is a privilege, not a right. This Acceptable Technology Use Policy codifies what is considered acceptable use of computers and the network. It is the policy of Vanguard to comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)] and prevent the following types of inappropriate user actions:

- Inappropriate material via the internet and electronic communication;
- Unauthorized access and unlawful activity; and
- Unauthorized disclosure, use, or dissemination of personal identification of minors.

For continued access to technological resources at school, adherence to the following policy is required.

Definitions

- **Harassment**: to disturb persistently; torment, as with troubles or cares; bother continually; pester; persecute
- **Defame**: to attack the good name or reputation of, as by speaking, portraying, or publishing maliciously or falsely anything injurious; slander or libel
- **Intellectual Property**: The ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person's intellectual property may involve royalty payments or permission but should always include proper credit to the source.
- **Plagiarism**: the unauthorized use or close imitation of the language and thoughts of another author and the representation of them as one's own original work
- **Technology Protection Measure**: a specific technology that blocks internet access to visual depictions that
    (a) are **obscene**: as the term is defined in section 1460 of title 18, United States Code, or
    (b) are **child pornography**: as the term is defined in section 2256 of title 18, United States Code, or
    (c) are **harmful to minors**

Acceptable Uses

- Students and staff will use the computers and networks solely for educational purposes. Acceptable uses include, but are not limited to, the following:
- Course Assignments
    - Students and staff may use school software and the internet to assist them in completing course research.
    - Students and staff may only access web pages using school computers and networks for specific educational objectives as directed by teachers and/or administrators. Content on websites must be related to educational activities.
- College Planning
    - Students may provide personal contact information to education institutions for educational purposes and career development purposes.

Individual Interests

- Students may access school computers during their study periods. Students who are using computers for assignments take priority over those who are using computers for individual interests. Acceptable uses include, but are not limited to, reading an online newspaper, practicing typing skills, computer programing practice, and photography editing.

Students and staff are expected to obey the rules of network etiquette. These rules include, but are not limited to the following:

- Be polite.
- Never send or encourage others to send abusive messages.
- Use appropriate language.
- Use electronic mail correctly (i.e., no sales, advertisements, solicitations, etc.)

Unacceptable Uses

To the extent possible and practical, steps shall be taken to support the safety and security of users of the network and direct electronic communications at Vanguard. Unacceptable uses include, but are not limited to, the following:

- Students and staff will not post information that could cause damage, danger, or disruption to another person.
    - Students and staff will not engage in personal attacks or harass another person.
    - Students and staff will not knowingly or recklessly post false or defamatory information.
    - Students and staff will not use speech that is inappropriate in an educational setting or violates school rules.
    - Students will not share personal contact information about themselves or other people.
    - *Personal contact information* includes your name, phone number, address, email address. *(see exception in **Acceptable Uses**)*

- Students and staff will not use technology resources for non-educational purposes.
    - Students and staff will not use technology resources for commercial uses or political lobbying.
    - Students will not use technology resources for social networking including, but not limited to, chatting or instant messaging, Facebook, Instagram, Snapchat, and Twitter.
- Students and staff will not be disrespectful of others' privacy and property.
    - Students and staff will not log in to another person's account. If another account is open, it is one's responsibility to log out of the account and log back in with his or her username and password.
    - Students and staff will respect the intellectual property of others.
    - Students and staff will not plagiarize words found on the internet or from peers.
- Students and staff will not modify the computer or network.
    - Students and staff will not download software without permission from the IT Department.
    - Students and staff will not attempt to harm or destroy data, the network, hardware, or software.
    - Students and staff will not attempt to harm, bypass, or destroy internet filters.
    - Students will not modify any settings on public profiles, such as those on shared computers.

Computer Security

Security on school computer systems and devices is a high priority. Students and staff who identify a security problem while using the internet or electronic communications must immediately notify an IT staff member.

- Students and staff shall not:
    - Use another person's password or any other identifier
    - Leave their password unprotected (for example, writing it down)
    - Leave their user accounts logged in at an unattended and unlocked computer
    - Connect, or attempt to connect, any personal devices of any kind to the school internal network (not WiFi) without prior knowledge and authorization of the IT Department

Personal Devices

Securing school information while allowing users to connect their personal devices on the network is still a major challenge. Personally owned devices may be used to access Vanguard resources as necessary in the course of normal daily routines in support of Vanguard goals and objectives. Users agree to a general code of conduct that recognizes the need to protect confidential data that is stored on, or accessed, using a personal device:

- Following all acceptable use policies and procedures as outlined in this document
- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining the software configuration of the device – both the operation system and the applications installed
- Ensuring a device's security controls are not subverted via hacks, jailbreaks, or security software changes
- Reporting a lost or stolen device immediately
- A support need or issue related to a personally owned device is the responsibility of the device owner except for Wi-Fi and web-based email access.

Accounts and Files

- Students and staff have their own accounts to gain access onto school computers.
- When saving, students and staff should save all information to their individual account. (Save in *My Documents* when logged into your account or save files in *OneDrive*.)
- At the end of each school year, all files on the student's account will be cleared. It is the student's responsibility to save any information they would like to keep to their own storage device before the last day of the school year.

Education, Supervision, and Monitoring

It shall be the responsibility of all members of the Vanguard staff to educate, supervise, and monitor appropriate access and usage of computer and network use as outlined below:

- Students may only access computers when there is a staff member present.
- For use of the computer labs, a staff member has agreed to allow students access to the lab for educational purposes and is responsible for checking on the students periodically. Refer to the Mobile Lab Policy for specific guidelines on reserving and using the labs.
- For use of the library computers, a librarian or staff member must be present. It is the responsibility of any staff members present to periodically check student use of computers.

Organizational Responsibility

It is impossible for Vanguard to restrict access to *all* controversial materials. The school does not have complete control over the accuracy of information on the internet or the effectiveness of filtering programs. Therefore, the school may not be held responsible for inappropriate communication on the network or for any objectionable material viewed or used by a student.

No Expectation of Privacy
Students and staff have no expectation of privacy in their use of school computers. The IT Department can monitor, inspect, copy, review, and store (at any time, without prior notice) all internet usage and electronic communications. All material and information accessed/received through computer systems and devices shall remain the property of Vanguard.

Children's Internet Protection Act (CIPA)
Per CIPA, The Vanguard School has adopted the necessary measures to ensure its compliance with the federal law. Compliance includes the following components:

- **Technology Protection Measures:** internet filters to block/filter internet access to visual depictions that
  (a) are obscene, or
  (b) are child pornography, or
  (c) are harmful to minors
- **Internet Safety Policy**
  - Restricting access to inappropriate material on the internet
  - Ensuring the safety and security of students and staff when using direct electronic communications
  - Addressing unlawful activities including "hacking"
  - Addressing unauthorized disclosure, use, and dissemination of personal information
- **Public Meeting and Reasonable Public Notice**: The school will hold a public meeting in which the technology protection measures and internet safety policy are addressed.

Penalties for Improper Use
Consequences for violating the Acceptable Technology Use Policy shall be decided by school administrators on a case by case basis. Potential consequences include, but are not limited to:

- Use of computer under direct supervision
- Suspension of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school
- Termination of employment
- Legal action

When questionable usage has taken place, it is the student's and/or staff member's responsibility to inform the IT Department. Not doing so may lead to further consequences.