

Internet Safety and Electronic Devices

Acceptable Use Policy

Venture Academy and Venture High School recognize the need for a policy governing the use of the electronic information resources and devices by students or staff, volunteers and board members (hereafter “staff”) as outlined in Utah State Code 53A-3-422 and R277-495. Responsibility is delegated to the Administration for implementing the policy according to established guidelines.

Electronic information resources will be available to qualifying students at Venture Academy. These resources include access to the internet and other network files or accounts. Our goal in providing electronic services to students and staff is to promote educational excellence by facilitating resource sharing, innovation, and communication.

Venture Academy has expectations established for appropriate use of existing and emerging technologies which students and staff may possess, including but not limited to cellular phones, digital picture/video cameras and/or camera phones, and other personal electronic devices capable of transmitting data or images through a wireless connection.

Administration Policy

Student and staff use of electronic information resources must be in support of education and research and must be consistent with the educational objectives of Venture Academy. While access to all materials on a worldwide network cannot be controlled, internet access at Venture Academy is filtered and monitored on an ongoing basis.

Internet resources can be valuable for a student’s education. School internet access is a privilege which may be authorized as well as withdrawn. Staff is subject to this policy and will be responsible for following and enforcing it. If students, staff, or other stakeholders have complaints about the policy, its enforcement, or about observed behavior, they are encouraged to inform administration. The administration will investigate and take the necessary course of action as related to this policy.

Personal Safety and Privacy

Personal contact information may not be shared on internet sites open to public access. This includes student or staff addresses, phone numbers, social security numbers, and personal email addresses unless authorized for educational purposes. Entering or otherwise disclosing personal information of other students or organizations is strictly prohibited. Students and staff shall not disclose personal information about themselves or others on websites, social media platforms, or in any online communication without permission from a teacher or guardian.

Internet Safety and Electronic Devices

Acceptable Use Policy

Internet Use

Students and staff may use school internet access to **utilize digital tools, including AI**, in a responsible, ethical, and legal manner only for educational purposes as directed by teachers and administration. **Many tools available on the internet offer potential benefits for education as well as risks that must be thoughtfully managed.** Students and staff are obligated to follow all rules established by teachers and administration regarding the use of the internet for various educational purposes.

Students or staff who formally publish school related information on the internet must first inform a teacher or administration and have appropriate permission, teacher supervision and approval by Venture Academy to do so.

Content Filtering

All content is filtered for inappropriate material by a network appliance. Filtering includes, but is not limited to, obscene, explicit, or harmful material as required by CIPA (Children's Internet Protection Act). The filtering software and configurations shall be audited and updated at least quarterly to ensure their effectiveness in blocking inappropriate content. Any attempts to bypass or disable the filtering software are strictly prohibited and will result in disciplinary action.

Prohibitions

In conjunction with content filtering, students and staff are strictly forbidden from:

- Accessing, creating, or transmitting material that is illegal, inappropriate, or disruptive to the educational environment.
- Accessing protected files or materials on the school network without authorization or attempting to obtain unauthorized access to online materials by hacking or other unlawful means.
- **Creating, accessing, or directing generative AI to produce** offensive, profane, or pornographic files, or similarly inappropriate material. If inappropriate material is accessed unintentionally, students must let their teacher know immediately.
- Engaging in cyberbullying activities defined as any electronic communication **(including AI generated output)** that has the purpose or effect of creating an intimidating, demeaning, humiliating, or hostile environment. In such cases where cyberbullying takes place outside of school or school-sponsored events, but is reported to school officials, the report will be turned over to the proper authorities (e.g., parents/guardians, or if unlawful behavior is suspected, law enforcement officials.) Any such cyberbullying activity shall be reported to administration immediately. The school reserves the right to judge the threat to student safety that any of these

Internet Safety and Electronic Devices

Acceptable Use Policy

outside of school situations present, and to apply disciplinary action up to and including suspension and expulsion.

- Inputting personal, sensitive, or confidential data into any online system, website, AI tool, etc., without prior authorization, including any data related to student educational records.
- Using Internet games such as MUDs (Multi-user domains), MMOs (Massively Multiplayer Online games) IRCs, or other such internet applications and resources unless specific permission has been granted by teachers or administration.
- Using internet enabled glasses (eyewear) or other wearable devices is prohibited as their use cannot be reasonably or responsibly monitored in a way that meets the requirements of this policy.
- Using internet sites and applications (e.g., online chat sites) which may seriously compromise the user's safety and security.
- Plagiarism, copyright violations, and trademark infringement cover copying another's work, digital copy-pasting, as well as the misuse of AI-generated materials. Students are required to use proper citations whenever incorporating ideas, words, or media from others. Teachers will clarify when and where AI tools can be used appropriately in their respective classrooms. Utilizing AI to complete assignments or generate answers outside of these approved parameters is considered cheating; likewise, presenting copied work or AI-generated output as one's own original work is considered plagiarism.
- Attempting to bypass computer security, or gain unauthorized access (i.e., hacking).
- Using electronic devices during standardized assessments unless specifically allowed by statute, regulation, student IEP, or assessment instructions.

Expectation of Privacy

Students and staff do not have an expectation of privacy in files, disks, documents, internet history, etc., which have been used or created at the school or with Venture Academy equipment.

The school reserves the right to monitor and review internet usage and network activity to ensure compliance with this policy and to maintain a safe and secure environment.

In addition, in compliance with state and federal law, students and staff have a limited expectation of privacy on the school's network and internet system resources. Routine monitoring or maintenance may lead to discovery that a user has violated school policy or law. Also, individual targeted searches will be conducted if there is reasonable suspicion that a user has violated policy or law. Personal electronic

Internet Safety and Electronic Devices

Acceptable Use Policy

devices of any student or staff suspected of violation of the above policy will be confiscated for investigation and may be turned over to law enforcement.

Any violations of this policy may result in disciplinary action, including but not limited to warnings, loss of internet privileges, or legal action if necessary.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy property of the school, another user or of any other agencies or networks that are connected to the network or the internet system. Vandalism also includes, but is not limited to: abusive overloading of data on the server or the uploading, downloading or creation of computer viruses. Any engagement in network vandalism constitutes unacceptable use and will subject the student to appropriate disciplinary action.

Student Responsibility

Students are personally responsible for devices assigned or provided to them by Venture Academy, both for loss or damage of devices and use of devices consistent with LEA directives.

Staff Responsibility

School staff members are expected to reasonably monitor student internet use during school hours and ensure compliance with this policy. They are expected to promote and model responsible and safe internet use. Staff members should promptly report any violations of this policy to administration.

Security

Security on any computer system is a high priority because of multiple users. Do not use another individual's account or any other login other than your own at any time. Any security concern must be reported to the principal, teacher/supervisor or systems administrator.

Disciplinary Actions

The use of electronic information resources is a privilege, not a right. Inappropriate use of these resources will result in suspension of privileges, and/or disciplinary action (including the possibility of suspension or expulsion), and/or referral to legal authorities. The principal, teacher/supervisor or systems administrator may limit, suspend or revoke access to electronic resources at any time which may result in missed assignments, inability to participate in required assessments, and possible loss of credit or academic grade consequences. The use of electronic devices in violation of Venture Academy

Internet Safety and Electronic Devices

Acceptable Use Policy

or teacher instructional policies may result in the confiscation of personal devices for a designated period.

Online Safety

As part of Venture Academy's ongoing effort to provide internet safety, students are educated about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms and cyberbullying awareness and response.
