ACCEPTABLE USE POLICY FOR TECHNOLOGY AND INTERNET PROTECTION POLICY

Introduction

CVES provides students, employees and guests (users) ready access to technology to assist learning and teaching, improve communications, simplify administrative tasks and promote research. CVES networks and/or technologies are resources that provide Internet, e-mail, as well as access to relevant software, printing and data storage in a secure environment.

To help fulfill these objectives, CVES has adopted this Acceptable Use Policy for Technology (AUP). The AUP is a series of guidelines covering technology use for users. Users are expected to adhere to this policy. Failure to do so can result in disciplinary action, including but not limited to, suspension of access to the CVES networks and/or technologies.

Privacy

CVES networks and technologies are property of CVES and their use is subject to CVES policies. All Users waive all rights to, and expectation of, privacy while using the networks and/or technologies, including but not limited to the following:

- CVES has the right to monitor all aspects of the CVES networks and/or technologies, including but not limited to, data saved on CVES networks and technologies owned by CVES; monitoring of sites accessed through the CVES networks and/or technologies; and reviewing e-mails sent or received by Users on CVES networks and technologies.
- By acceptance of the right to access the CVES networks and technologies, Users waive all privacy rights to or in anything created, stored, reviewed, sent or received on CVES networks and/or technologies.

Recording on Campus or CVES sponsored activities

Secret Recordings

No students, employees, or guests shall make secret audio or video recordings of people, or activities on CVES campus or CVES sponsored events, without the prior approval of District Administrator, District Superintendent, or CVES Board of Cooperative Educational Services. Such approval shall only be granted for the purposes of physical security or investigation or enforcement of law, regulation or policy or procedure of CVES. For the purposes of this paragraph, secret means not readily apparent to a nearby observer.

Non Public Events

No one shall make audio or video recordings of spaces or events which are not open to the general public without prior approval of the CVES personnel responsible for supervising the space or activity in which the recording shall occur.

Public Events
Events which are open to the public, such as open houses, sporting events, concerts, and the like, may be recorded so long as the method of setting up or recording the event is not disruptive and does not violate other CVES rules.

For the purposes of this subdivision "recordings" include video and photographic snapshots as well as moving pictures.

General Use

The use of CVES networks and/or technologies generally conforms to the same standards and procedures as other types of CVES-owned equipment. Because of the unique capabilities of technologies, particularly as it relates to security, there is a need for the additional guidelines stated below:

- All computers in the District having internet access which students have access to shall be subject to filtering software in accordance with the Federal Children's Internet Protection Act. (CIPA).
- Users will adhere to, and be subject to, the terms of all relevant federal, state and local laws related to networks and/or technologies use.
- Users are prohibited from the unauthorized accessing, modifying, deleting, pirating or vandalizing of data or software on CVES networks and/or technologies.
- Users are prohibited from using CVES networks and/or technologies for harassment, threats, bullying and defamation of others.
- Users will use CVES networks and/or technologies for educationally valid, CVES-related purposes only. This applies to both on- and off-campus.
- Users are expected to handle all CVES technologies with care and may be held responsible for any replacement or repair costs.
- Users will not attempt to fix CVES networks and/or technologies or install software or hardware of any kind. Instead, they must initiate a service request through the CVES Technology Department.
- Users should be aware that only software approved by the CVES technology department in consultation with the immediate supervisor, can be installed on CVES networks and/or technologies.
    - Users interested in obtaining software for instructional or professional use, must initiate a request for purchase through the immediate supervisor.
    - Users interested in obtaining free software for instructional or professional use, must initiate a service request through the CVES Technology Department
- Users will not relocate CVES printers, computers, interactive white boards, fixed projectors without the approval of the immediate supervisor in consultation with the CVES technology department; such moves should be reported to the Business Office in order to maintain the accuracy of the Fixed Assets Inventory.
- Users will follow divisional protocols for signing out portable technologies.
- Users shall not circumvent any CVES networks and technologies security measures imposed by CVES or non-CVES organizations.

- Personal files should not be stored on CVES network and technologies; any such files may be deleted at any time.

Internet Use and Safety

The Internet offers students and staff innumerable possibilities for learning, research and communication over a wide spectrum of topics and media formats. However, because the Internet is a global network with minimal external controls, it is impossible to control what information users may locate and attempt to utilize. This information can be pornographic, violent, hateful, inaccurate, false or simply educationally irrelevant. For these reasons, CVES cannot verify, or be responsible for, the accuracy and/or content of the information found on the Internet. CVES is committed to comply with state and federal laws regarding student online activity and privacy, including FERPA and CIPA.

While CVES utilizes filtering software, it cannot warrant that there will not be interruptions in protection due to temporary breakdowns or limitations in the effectiveness of the filtering technology. Therefore, in order to further protect users, to provide them with relevant educational experiences, and to ensure that time is used for educational or work-related purposes, the following guidelines are established:

- Users are prohibited from accessing sites or distributing content which is pornographic, obscene, promotes violence or advocates destruction of property, including information concerning the manufacture of destructive devices, such as explosives, fireworks, smoke bombs, incendiary devices or the like; illegal, gambling, even in cases where filtering does not block access, unless for educational purposes approved by immediate supervisor in consultation with the CVES technology department. When filtering does not block access, it must be reported immediately to the CVES technology department.
- Users are prohibited from accessing, transmitting or retransmitting material which advocates or promotes violence or hatred against particular individuals or groups of individuals or advocates or promotes the superiority of one racial, ethnic or religious group over another.
- Students are prohibited from CVES Networks and Technologies to access an instant messenger service or program, Internet Relay Chat, Facebook, Twitter, or other social media site or other forms of direct electronic communication, or enter a chat room.
- Users are not allowed to download non-educationally valid materials, including but not limited to documents, photos, videos, or music.
- Users are only permitted to use CVES approved file sharing software to download, share or distribute including but not limited to music, video, picture, data or program files.
- Users are only permitted to use CVES approved cloud storage.
- Employees are only permitted to enter Confidential or Personally Identifiable Information to CVES approved: cloud storage, Student Management Systems, and other websites.

E-mail Use

E-mail is a primary method of communication to provide timely information. Excessive e-mail traffic can take up limited disk storage. Hackers use e-mail as a vehicle for introducing virus and perpetrating hoaxes. Equally important, having to read and dispose of large quantities of irrelevant, unsolicited e-mail, referred to as junk mail or spam, can be an annoyance and a waste of productive time to employees.

- Students are not provided with individual e-mail accounts.
- Email is regular method of communication between CVES and its staff. Employees shall check their e-mail regularly.
- Employees are provided e-mail in order to more easily communicate with their colleagues, inside and outside CVES, on organization-related matters only.
- Employees should immediately delete suspicious e-mails, even if it appears to have been sent from someone they know. They should also report it to CVES Technology Department.
- All e-mails are filtered. If an expected e-mail has not arrived, employees should initiate a service request through the Technology department.

Employee Responsibilities Regarding Student Use

It is the responsibility of employees to protect students from objectionable materials, and provide them with relevant and rewarding educational experiences.

- Employees must supervise students in the safe and proper use of any CVES network and technologies.
- Employees must monitor the Internet content that students are accessing.
- Parents/Legal Guardians will be provided a copy of this Acceptable Use Policy on a yearly basis and will be encouraged to contact employees to discuss these procedures if they have any questions.
- Employees must provide students education about safe and proper use of technologies.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access.

- Employees and students shall not reveal their passwords to any unauthorized individual.
- Users will not leave their system unattended while they are logged on. Any unauthorized use of a user account must be reported to their immediate supervisor.
- Unauthorized access is strictly prohibited.
- Passwords will follow guidelines set forth by the Technology Department.

Removable Media Use

All removable media such as but not limited to DVDs, CDs and USB-based memory drives – also known as flash drives, key drives and thumb drives – are highly convenient tools. Their convenience can potentially expose CVES to additional risk, as these devices are easily lost or otherwise compromised.

- Users may utilize Removable Media on CVES Network and Technologies for educationally valid materials.
- Users utilizing Removable media for any Confidential or Personally Identifiable Information must securely protect with a password and/or are encrypted to ensure the safety of the data.

Personal Device Use

The use of personal devices in the classroom can add educational value when such devices deliver content and extend, enhance or reinforce the student learning process.

- Classroom teachers determine the appropriateness of in-class use of personal devices, consistent with district instructional objectives, and with approval of the divisional director.
- Users needing Internet Access for their personal device may only utilize the CVES Portal Wireless Network.
- Users may not use any personal device in a manner that is disruptive to any other user.
- CVES is not responsible for any damage to the personal device.
- Users may be held responsible for any replacement or repair costs caused by their personal device.
- Users may only connect a personal device to CVES Technologies with prior authorization.

Disciplinary Consequences and Procedures

Users who use CVES networks and/or technologies are expected to comply with this policy in its entirety as well as with any administrative regulations adopted in furtherance of this policy. The District Superintendent is authorized to implement administrative regulations in furtherance of this policy which would include a discussion of the possible suspension of Users access right to CVES networks and/or technologies and the possibility of appropriate disciplinary action.

Student Violations

First Violation:
Upon confirmation of the first violation of the AUP, disciplinary consequences and procedures will be determined as outlined in the CVES Code of Conduct. A violation action letter will be sent home with the student. The student's parent/guardian must sign and return this letter. In addition to any disciplinary consequences imposed, the student's home school will be notified of the violation and, depending on the severity of the violation, the student's Internet access may be temporarily suspended or terminated for the remainder of the school year. Access to the Internet will not be reinstated at any time unless the violation action letter has been signed by the student's parent/guardian and returned to CVES.

Second Violations:
If there is a second AUP violation by the same student during the school year, the student's Internet access will be temporarily suspended or terminated for the remainder of the school year. The student's home school will be notified of the violation, and a second violation action letter will be generated and sent home with the student. The student's parent/guardian must sign and return this letter. In addition to any disciplinary consequences imposed, depending on the severity of the violation, the student's access to other CVES networks and technologies may also be temporarily suspended or terminated for the remainder of the school year. Access to the Internet and other CVES networks and technologies will

not reinstated at any time unless the violation action letter has been signed by the student's parent/guardian and returned to CVES.

Subsequent Violations:
Any further violation of the AUP by the same student during the school year will result in a meeting between the student, parent/guardian, teacher, and the division head. The division head will at that time determine whether the student's access to all CVES network and/or technologies will be terminated, including the duration of such termination. The student's home school will be notified if access to CVES networks and technologies is terminated.

In addition to the above consequences, students shall be subject to disciplinary consequences and procedures will be determined as outlined in the CVES Code of Conduct for violations of the acceptable use policy.

Special Circumstances

There may occur special circumstances that require permission to access resources or otherwise use technology in a way that would normally be considered in violation of the CVES AUP. Any such situation will be evaluated on a case-by-case basis, and exceptions to the CVES AUP will be at the discretion of the CVES Technology Department or District Superintendent. In those cases, any such action will be carried out or supervised by the CVES Technology Department in order to insure the safety and security of CVES networks and technologies, and to assure that such action is carried out in an appropriate manner. When this procedure is followed, such instances will not be considered violations of the CVES AUP.