

**CLINTON-ESSEX-WARREN-WASHINGTON BOCES**  
**CHAMPLAIN VALLEY EDUCATIONAL SERVICES**

# **Acceptable Use Policy For Technology Resources**

**Public Non-Discrimination Notice:**

Clinton-Essex-Warren-Washington BOCES a/k/a/ Champlain Valley Educational Services (CVES) hereby advises students, parents, employees and the general public that it offers educational and employment opportunities without regard to sex, race, color, national origin, creed or religion, marital status, age, gender preference or disability. Students shall not be excluded from participation in, be denied the benefits of, or otherwise be subject to unlawful discrimination under any program or activity. Inquiries regarding this nondiscrimination policy may be directed to:

James McCartney – Title IX Compliance Officer

Cathy Snow – Title IX Compliance Officer

1585 Military Turnpike

P.O. Box 455, Plattsburgh, NY 12901

Phone: 518-561-0100 Ext. 236

Roxanne Pombrio – Section 504 Compliance Officer

1585 Military Turnpike

P.O. Box 455, Plattsburgh, NY 12901

Phone: 518-561-0100 Ext. 299

**Adopted 8/17/11**

## Acceptable Use Policy For Technology Resources

### TABLE OF CONTENTS

Introduction .....	1
Responsibility When Using Technology Resources.....	2
Use of laptops and Other Electronic Devices.....	2
Acceptable And Unacceptable Use of All Technology Resources .....	7
Copyright and Use.....	9
Interpretation .....	9
Consequences of Misuse .....	9
Special Circumstances .....	11
Vandalism / Abuse / Theft .....	12
Internet Filtering .....	12
Privacy and Security .....	12
Reliability and Limitation of Liability .....	13
Definitions .....	14

**CLINTON-ESSEX-WARREN-WASHINGTON BOCES**  
**CHAMPLAIN VALLEY EDUCATIONAL SERVICES**  
**Acceptable Use Policy For Technology Resources**

The purpose of this document is to inform staff, students, parents, guardians, and guests of the rules governing the use of district and personal technology resources and to set expectations of privacy while using those resources on or near Champlain Valley Educational Services (CVES) property, in CVES vehicles and at CVES sponsored events. This document shall be used in conjunction with the CVES Code of Conduct and all other CVES policies.

**Introduction**

The purpose of CVES is to be a leader in providing quality, cost-effective programs and services that support school districts and their communities to achieve higher standards through enhanced educational opportunities. To fulfill this institutional mission, CVES and its students, staff, and guests must carry on countless day-to-day operations and interpersonal communications through the use of technology. Equally necessary at an educational institution is free speech and the sharing of materials and ideas that advance the cause of learning and mutual understanding. CVES offers access to district computers, communications systems, the Internet and an array of other technology resources to promote educational excellence. Each user is responsible for her/his use of technology, whether personal or district-provided. While using district and personal technology resources on or near CVES property, in CVES vehicles, and at CVES-sponsored events, each user must act in an appropriate manner consistent with CVES and legal guidelines.

At the beginning of the school year, a signature packet will be sent home with each student, including copies of the CVES Acceptable Use Policy (AUP) and Media Release Form. These forms must be signed by all students as well as their parent(s)/guardian(s), and must be renewed on an annual basis. All staff will sign these forms upon employment or revision of the policy. New students and staff entering CVES after this time must sign these forms as part of their registration or intake process. Access to technology resources will be denied without a signed AUP Signature Form or guest account agreement. Staff signature packets will be filed in the CVES Human Resources office. Student packets will be the responsibility of the teachers and filed in accordance with division policy. Guest agreements will be submitted to the division technology staff or the division office and then forwarded to the CVES Technology Department prior to each use.

Guests must read the CVES Acceptable Use Policy and sign an Technology Resources for Education Guest Account Agreement. Access to technology resources will be denied without a signed Guest Account Agreement.

Guests who are identified as visiting school district personnel, as defined in the Definitions section of this document, must have a signed acceptable use policy agreement on file with their home district to access CVES technology resources. Any such guest must agree to abide by not only their home district AUP, but the CVES AUP and CVES Code of Conduct as well.

CVES reserves the right to modify the terms and conditions of this document at any time. The latest version of this document is available on the CVES web site at <http://www.CVES.org/aup>

## **Responsibility When Using Technology Resources**

The educational value of technology integration in curriculum is substantial. CVES technology resources are provided to deliver and enhance curriculum and assignments, conduct research, complete assignments, and communicate with others in furtherance of education or carrying out student coursework, staff employment duties, and other educational purposes. Any and all use of CVES networks or technologies is subject to the terms of the CVES Acceptable Use Policy and CVES Code of Conduct. Access is a privilege, not a right. As such, general rules of behavior apply.

### **Student Responsibility**

It is the joint responsibility of CVES personnel and the parent or guardian of each student to educate the student about his/her responsibilities, and to establish expectations when using technology. Ultimately, parents or guardians are responsible for setting and conveying the standards that their children should follow when using technology. During school, teachers will model and instruct students on the appropriate use of technology and resources. It is the responsibility of individual students to act responsibly and to follow teacher directions and CVES guidelines when using CVES or personal technologies.

Access to technology is given to students who agree to act in a considerate and responsible manner. Just as students are responsible for good behavior in a classroom or a school hallway, they must also be responsible when using CVES or personal technologies. Students must comply with CVES standards, as well as the CVES code of conduct, and honor the CVES AUP to be permitted the use of technology.

### **Staff and Guest Responsibility**

It is the sole responsibility of individual staff and guests to educate themselves about their responsibilities, to act responsibly and professionally, and to follow CVES guidelines when using CVES or personal technologies.

Furthermore, teachers will model and instruct students on the appropriate use of technology and resources, including proper care of equipment, file management, search strategies, user safety, copyright laws, and computer etiquette.

Access to technology is given to staff and guests who agree to act in a considerate, professional, and responsible manner when using CVES or personal technologies. Staff and guests must comply with CVES standards, as well as the CVES code of conduct, and honor the CVES AUP to be permitted the use of technology.

## **Use of laptops and Other Electronic Devices**

Students, staff, and guests are expected to follow all CVES policies and honor the CVES AUP when using personal and CVES laptops, electronic devices, and associated equipment.

### **Personal Laptop Use**

Students, staff, and guests may only use personal personal laptops at CVES where there is a bona-fide educational requirement to do so and such use is at the discretion of the CVES Technology Department with input from the division director.

The following guidelines are provided to manage the use of personal laptops and associated equipment:

- The owner of the laptop is solely responsible for how the laptop is used regardless as to whether the owner or a borrower of the laptop is performing actions on it.

- CVES will not be held responsible for hardware or software problems, infection, data loss, or damage resulting from use of personal laptops devices on CVES property.
- The owner of the laptop is solely responsible for the security of the laptop, any damages to the laptop, and damages the laptop may cause to CVES equipment to which it attaches (networks, projectors, other computer equipment, etc.).
- The laptop must be running the most current version of a virus protection software package approved by the CVES Technology Department, including the latest weekly virus definition files.
- The laptop must be up to date with the most current security patches for its operating system.
- The laptop is free of spyware, adware, worms, viruses, trojan horses, and peer to peer software.
- The laptop must not be running any Internet or web hosting services and must not have Internet Connection Sharing, File Sharing, or Printer Sharing services turned on.
- Connection of personal laptops to CVES computers or network or Internet resources is not permitted for staff or students.
- Connection of personal laptops to CVES computers or private network resources is not permitted for guests. However, when there is a bona-fide educational requirement for guests to have Internet access, at the discretion of the the CVES Technology Department with input from the division director, the user will be provided a designated Ethernet port to attach the device. In the limited areas at CVES where there is wireless network access, it is at the discretion of the the CVES Technology Department, with input from the division director, to grant use of such access.
- Guests and all users of the guest's personal laptop must request network access prior to each use of their laptop by reading the CVES Acceptable Use Policy and signing an Acceptable Use For Technology Resources Guest Account Agreement. This form will be submitted to the division technology staff, or submitted to the division office and then forwarded to the CVES Technology Department.
- A "use" is the authorized period defined on the Acceptable Use For Technology Resources Guest Account Agreement. Under normal circumstances, that period will be from one day to one week. Periods exceeding one week may be approved only after discussion between the division director and the CVES Technology Department. Access will only be granted at the discretion of the CVES Technology Department with input from the division director, in circumstances where there is a bona-fide need that benefits CVES.
- Reasonable printing of class assignments and work related documents is permitted, but must be done from a CVES computer using a personal portable storage or data-transfer device compatible with CVES equipment. It is the owner's responsibility to have a suitable device.
- CVES is unable to supply or install software on personal laptops due to legal constraints and licensing agreements.
- CVES cannot provide technical assistance for hardware or software problems that may occur with personal laptops and associated equipment. Such assistance remains the personal responsibility of the owner. The CVES Technology Department has a responsibility to maintain CVES technology equipment and is unable to respond to private needs.
- The appropriateness of laptop use by students remains at the discretion of the teacher. In the event of students using their laptop inappropriately, the teacher may require the student to shut down the computer and continue working via other means, take disciplinary action, or both using the same procedures as if the violation had occurred while using CVES equipment.

- CVES staff may confiscate and temporarily hold (pending parental or same-day student pick up) personal laptops that are used inappropriately while in the possession of a student.
- Where there is reasonable suspicion that material in violation of the Acceptable Use Policy is being brought to CVES on a personal laptop by a student, staff or guest, CVES reserves the right to ban the laptop from campus grounds and impound the computer.

### **Personal Electronic Devices**

- Any individual who possesses a personal electronic device shall be solely responsible for its care and security.
- CVES will not be held responsible for hardware or software problems, infection, data loss, or damage resulting from use of personal electronic devices on CVES property.
- The CVES Code of Conduct permits students to possess such devices during the school day. It also states that students are prohibited from using or having on or in an operational mode any type of personal electronic device during the school day, except as expressly permitted in connection with authorized use, and that students are prohibited from using them in any manner which disrupts the educational environment or process. These devices must be kept out of sight and powered off or silenced during the school day.
- Staff and guests are permitted to have and use personal electronic devices during the school day, but are prohibited from using them in any manner which disrupts the educational environment or process. Staff are expected to model appropriate use for students by keeping these devices out of sight and powered off or silenced during the school day, while in the presence of students.
- It is the understanding of all staff that the CVES Technology Department will provide no technical assistance or support for personal electronic devices or their associated software and accessories.
- Connection of personal electronic devices to CVES computers is not permitted for staff, students or guests.
- Connection of personal electronic devices to CVES private network resources is not permitted for staff, students or guests. Reasonable printing of class assignments and work related documents is permitted, but must be done from a CVES computer using a personal portable storage or data-transfer device compatible with CVES equipment. It is the owner's responsibility to have a suitable device.
- No individual shall use personal electronic devices on school property in any way that would violate any CVES policy or rule, or any federal, State, or local law or regulation.
- The appropriateness of device use by students remains at the discretion of the teacher. In the event a personal electronic device is used inappropriately by a student, the teacher may require the student to shut down the device and continue working via other means, take disciplinary action, or both using the same procedures as if the violation had occurred while using CVES equipment.
- CVES staff may confiscate and temporarily hold (pending parental or same-day student pick up) personal electronic devices that are used inappropriately while in the possession of a student.

### **CVES Owned Laptops and Electronic Devices**

CVES allows staff, students and guests to use CVES laptops inside and outside the school in order to enhance, enrich, and facilitate teaching and administrative duties as well as for CVES communications.

CVES laptops are only to be used as a productivity tool for CVES related business, curriculum enhancement, research, and communications.

All laptops and related equipment and accessories are CVES property and are provided to staff or students for a period of time as deemed appropriate by the CVES Technology Department, with input from the division director. As a condition of their use, staff and students must comply with and agree to all of the following:

- Prior to using CVES laptops or electronic devices, staff, guests and students must sign the Laptop and Electronic Device Acceptance Form and agree to all terms and conditions as outlined. These forms will be submitted to the division technology staff, or submitted to the division office and then forwarded to the CVES Technology Department.
- Staff, students, and guests must NOT attempt to install software or hardware or change the system configuration including network settings without prior consultation and written consent of the CVES Technology Department. Any unauthorized software will be removed by the CVES Technology Department upon discovery.
- Staff, students, and guests are expected to protect CVES computer equipment from damage and theft, and are solely responsible for any damages or theft that occurs as a result of their own negligence or misuse.
- No user may hold CVES responsible for hardware or software problems, infection, data loss, or damage resulting from use of CVES owned laptops or electronic devices, whether on or off CVES property.
- If network or Internet access is needed, at the discretion of the the CVES Technology Department with input from the division director, the user will be provided a designated Ethernet port to attach the laptop or device. In the limited areas at CVES where there is wireless network access, it is at the discretion of the the CVES Technology Department with input from the division director, to grant use of such access. All users of the laptop or device understand that no workstation or other CVES equipment will be disconnected from the network in order to provide network or Internet access.
- Staff, students, and guests will not be held responsible for software problems resulting from normal CVES-related use; however, staff, students, and guests will be held personally responsible for any problems caused by their negligence or misuse as determined by CVES administration.
- Staff, students, and guests will promptly provide access to any laptop computer or electronic device, and associated equipment they have been assigned upon CVES request.
- Staff, students, and guests fully understand that such laptops, electronic devices, and associated equipment are the property of CVES. Therefore, CVES reserves the right to inspect laptops at any time it deems appropriate. Staff, students, and guests further understand they have no personal property rights in CVES laptops and electronic devices.

### **Laptops and Electronic Devices Belonging to Visiting School Districts**

CVES allows staff, students and guests to use visiting school district laptops and electronic devices inside and outside CVES in order to enhance, enrich, and facilitate teaching and administrative duties as well as for school related communications. As a condition of their use, staff and students must comply with and agree to all of the following:

- The owner and all users of visiting district laptops or electronic devices must have a signed Acceptable Use Policy agreement on file with their home district, or request to read the CVES Acceptable Use Policy and sign an Acceptable Use For Technology Resources Guest Account Agreement in order to connect to the Internet, or otherwise utilize CVES technology resources while on CVES property. Any Guest Account Agreements will be submitted to the division technology staff, or submitted to the division office and then forwarded to the CVES Technology Department.
- Any individual who possesses a visiting school district laptop or electronic device shall be solely responsible for its care and security.
- CVES will not be held responsible for hardware or software problems, infection, data loss, or damage resulting from use of visiting school district laptops or electronic devices on CVES property.
- Connection of visiting school district laptops or electronic devices to CVES computers is not permitted without authorization from the CVES Technology Department.
- Connection of visiting school district laptops or devices to CVES private network resources is not permitted. Reasonable printing of class assignments and work related documents is permitted, but must be done from a CVES computer using a portable storage or data-transfer device compatible with CVES equipment. It is the user's responsibility to have a suitable device.
- When there is a requirement for Internet access, the user will be provided a designated Ethernet port to attach the laptop or device. In the limited areas at CVES where there is wireless network access, it is at the discretion of the CVES Technology Department to grant use of such access. The owner and all users of the device understand that no workstation or other CVES equipment will be disconnected from the network in order to provide Internet access for the laptop or device.
- CVES cannot provide technical assistance for hardware or software problems that may occur with visiting school district laptops or electronic devices or associated equipment. The CVES Technology Department may assist users with configuration for use with the CVES network or other technology if it is deemed appropriate, and does not interfere with their normal duties.
- CVES is unable to supply or install software due to legal constraints and licensing agreements.
- The appropriateness of laptop use by students remains at the discretion of the teacher. In the event of students using a visiting school district's laptop inappropriately, the teacher may require the student to shut down the computer and continue working via other means, take disciplinary action, or both, using the same procedures as if the violation had occurred while using CVES equipment.
- CVES staff may confiscate and temporarily hold (pending visiting district or same-day student pick up) visiting school district laptops or electronic devices that are used inappropriately while in the possession of a student.
- Where there is reasonable suspicion that material in violation of the Acceptable Use Policy is being brought to CVES on, or accessed from a visiting school district laptop or electronic device while on CVES property, CVES reserves the right to ban the laptop or device from campus grounds and impound the laptop or device.

## **Acceptable And Unacceptable Use of All Technology Resources**

Users of CVES technologies are provided usernames and passwords to access various computers, systems, and other resources and are expected not to let other people use their accounts or reveal their passwords to others, except to CVES technology staff for purposes of assistance or systems administration.

All CVES technology resources, including but not limited to CVES computers, communications systems and the Internet, must be used in support of education or academic research and must be used in a manner consistent with the educational mission, objectives, and Code of Conduct of CVES.

### ***Acceptable Uses:***

**Activities that are permitted and encouraged when using CVES technologies and personal electronic devices on or near CVES property, in CVES vehicles, and at CVES sponsored events include:**

- Original creation and presentation of academic work.
- Student research on topics being studied in class.
- Staff research for curriculum and lesson plan development.
- Assignment and submission of work, using Moodle and other electronic formats.
- Researching opportunities for community service, employment or further education.
- Career development, using technology to apply, train, and prepare for employment.
- Approved use of educational webinars, forums, wikis, and blogs to communicate worldwide with students and educators and to utilize external educational resources.

### ***Unacceptable Uses:***

**Activities that are not permitted when using CVES technologies or personal electronic devices on or near CVES property, in CVES vehicles, and at CVES sponsored events include but are not limited to:**

- Using language that is inappropriate in an educational setting including, but not limited to obscene, profane, lewd, vulgar, rude, disrespectful, threatening, inflammatory, harassing, or involves personal attacks.
- Searching, viewing, communicating, publishing, downloading, storing, or retrieving materials that are inappropriate or not related to education or CVES job duties.
- Ordering any item, subscribing to any service, or submitting any request without division approval which in any way results in an unauthorized expense to CVES or that will cause anything to be shipped, mailed, e-mailed, faxed, telephoned or otherwise delivered to any address, residence, business, or CVES.
- Any access or use of any e-mail accounts that are not provided or authorized by CVES.
- Transmitting school materials for unethical purposes such as cheating.
- Plagiarism or representing Copyrighted ©, Registered ®, or Trademark <sup>TM</sup> materials as one's own work.
- Posting, sharing, or transmitting student or staff pictures or personal information in any type of media without division approval.

\* Staff may contact their division office to submit a request to post photos or personal information, and must verify that the applicable student or staff has a signed Media Release Form on file prior to posting. This applies to any student or staff who can clearly be identified in the media to be posted.

- Non-educational uses such as inappropriate games, gambling, shopping, personal banking, etc.

- Sending, replying, or forwarding chain letters, jokes, greeting cards, pyramid schemes, or any other item that could be considered “junk mail”.
- Accessing or participating in social networking sites.
- Student access of, or participation in, a chat, IM session, or other instant messaging site or service without the express authorization, approval and supervision of the instructor.
- Student participation, posting, commenting, or messaging on any forum, wiki, blog, or publicly editable site without the express authorization, approval and supervision of the instructor.
- Any staff assisting a student to violate any CVES policy, regulation, or law, regarding use of CVES technologies or personal electronic devices, or failing to report knowledge of such violations to the CVES Technology Department or administration.
- Using any type of electronic media to reveal, publicize, use, or reproduce confidential or proprietary information regarding CVES or its component districts including, but not limited to: financial information, databases, or the information contained therein, technology access codes or passwords, and staff or student personal information.
- Use of CVES resources for political lobbying, commercial purposes, personal financial gain, or fraud.
- Unreasonable or non-work related use of CVES printers and paper.
- Remotely accessing any computer or device, or using any form of cloud storage without written approval from the CVES Technology Department.
- Attempting to gain access to any computer, network, website, or service by using another person’s username or password, or allowing others to use yours.
- Damaging, modifying or hacking into CVES or external computers, networks, or other technology resources, including intentional or neglectful transmission of viruses or other destructive computer files.
- Attempting to bypass CVES Internet filters or any other security measures.
- Use of external storage devices, bootable CDs, portable OS, or other devices to alter the function of a computer or a network;
- Adding any software or applications to CVES computers, network or other technology, or modifying any existing software or applications, without written approval from the CVES Technology Department.
- Transmitting or receiving dangerous information, that if acted upon could cause damage, present a danger, or cause disruption.
- Criminal speech or speech in the course of committing a crime including, but not limited to threats to anyone including the President of the United States, instructions on breaking into computer systems, child pornography, drug dealing, gang activities, etc.
- Any activity that violates any CVES policy or rule, or any federal, State, or local law or regulation.

***All users are expected to report immediately any harassment, threats, hate-speech, or inappropriate content.***

- ***Students should report any such incident to a teacher.***
- ***Staff should report any such incident to the CVES Technology Department or administrator.***

## **Copyright and Use**

Users are forbidden from reading, publishing, changing, copying, deleting, downloading, or otherwise accessing files that they did not originally create, which are stored on CVES computer systems or network, unless specifically authorized to do so.

Installed software must be owned by CVES and/or properly licensed from the copyright owner thereof, and any modifications must comply with the terms of the applicable license(s). To insure compliance, any software that is used on CVES technology must be installed by the CVES Technology Department.

Credit should always be given to the person who created the article or is responsible for the idea. Take extra caution when using sources from the Internet. Cutting and pasting ideas into your own document, without giving credit to the author, is plagiarism. You must credit the source just as you would for any conventional hard copy source, using the following format:

Author; Title, (Full URL), Copyright Date.

*e.g., Smith, William; The Dawn of Time, (HTTP://www.anywhere.com/docs/dawn.htm), 1998.*

Users are cautioned that attempting to access, receive, stream, transmit, store, copy, or distribute any form of copyrighted material without written consent of the copyright holder, is a violation of the CVES AUP as well as U.S. copyright and/or patent laws. You should assume that any audio, video, software, document, or other file that you did not create and that is not specifically designated as in the public domain, or produced and distributed under a creative commons license, or in open broadcast to the public is copyrighted. As such, it is also a violation to access services that provide download, streaming, or private broadcast of such content, including but not limited to peer-to-peer networks such as limewire, kazaa, gnutella, etc.; audio services such as Napster, XM, Rhapsody, etc.; video services such as Netflix, Blockbuster, etc.

## **Interpretation**

Interpretation of the Acceptable Use Policy should be directed to the CVES Technology Department. If a student has any questions about whether a specific activity is permitted, or the meaning of any part of the CVES AUP he/she should ask a teacher. If staff or guests have any questions about whether a specific activity is permitted, or the meaning of any part of the CVES AUP he/she should ask the CVES Technology Department. Should additional questions arise, the division director or District Superintendent will be consulted by the CVES Technology Department to determine what constitutes appropriate use and the resulting decision will be final.

## **Consequences of Misuse**

Misuse of personal or CVES technology resources or personal electronic devices while on or near CVES property, in CVES vehicles and at CVES sponsored activities may result in suspended or restricted access to district technology and personal electronic devices, as well as disciplinary action up to and including long term suspension. CVES staff may confiscate and temporarily hold (pending parental or same-day student pick up) personal laptops or electronic devices that are used inappropriately while in the possession of a student.

If at any time a user is believed to be in violation of the Acceptable Use Policy, the CVES Technology Department may gain access to the user's e-mail and files for review including, but not limited to search and seizure of all necessary materials and property. If the incident involves a personal electronic device, the CVES Technology Department may search any confiscated personal electronic device belonging to a student, and examine the content of the device when there is reasonable suspicion of

unauthorized or illegal use of the device, and may turn the device over to the proper authorities for further investigation when warranted.

The CVES Technology Department, division directors, and the District Superintendent are responsible for the implementation and enforcement of the policies, rules, and regulations contained in this document.

Individual schools may choose to have additional rules and regulations pertaining to the use of personal, networked, and communications resources in their respective buildings, and all CVES students and staff are required to abide by them while at those schools. Furthermore, intentional unauthorized access or damage to networks, servers, user accounts, passwords, or other CVES resources may be punishable under federal, State, or local law.

### **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 Violation:**

If there is a second AUP violation by the same student during the school year, further disciplinary consequences and procedures will be determined as outlined in the CVES Code of Conduct and 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 technology resources may also be temporarily suspended or terminated for the remainder of the school year. Access to the Internet and other CVES technology resources 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.

#### **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 technology resources will be terminated, including the duration of such termination. The student's home school will be notified if access to CVES technology resources is terminated.

#### **Staff, Guest, and All Other User Violations:**

Any violation of the AUP will be addressed by the division director for appropriate action.

**Immediate Termination of Access:**

Some violations that may result in immediate termination of access for any user, or further action by CVES or federal, state, or local law enforcement include but are not limited to:

- Transmission of a threat.
- Transmission of spam e-mail.
- Any form of hacking, or attempt to bypass security measures.
- Any attempt to disrupt, degrade, disable, damage or otherwise interfere with normal or efficient operation of CVES networks or other technologies.
- Sending messages or accessing any technology or service using another user's identity.
- Violation of personal safety using technology.
- The creation, receipt, or transmission of sexually explicit, harassing, racist or terrorist material.
- Transmission of any material that endorses an illegal activity or violates any law or regulation.

If the CVES Technology Department determines that such a violation is in progress, or represents an imminent danger to any person, entity, CVES technology, the user's access to the Internet, network, accounts, or any other access with respect to technology may be immediately, and without notice terminated. Any action that may precipitate immediate termination of access will be addressed by the division director for appropriate action.

If any other staff observes that such a violation is in progress, he/she should immediately report the violation to their immediate supervisor and the CVES Technology Department.

**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.

While there is no way to anticipate all situations that would require such actions, some specific examples include, but are not limited to:

- Access of social networking or other prohibited sites to test or add certain blocking mechanisms in the firewall, Internet filtering, or other CVES system.
- Accessing personal e-mail to retrieve crucial information in the event of a CVES system or CVES e-mail delivery failure.
- Granting network or Internet access to a personal laptop or device to carry out a specific task or job duty that could not otherwise be reasonably completed.
- Access of social networking sites to investigate claims of cyberbullying.
- Assisting law enforcement in any investigation.

### **Vandalism / Abuse / Theft**

Any intentional act that damages CVES technology hardware, software, operating systems, or data will be considered vandalism. Any intentional act that requires a person's time to repair, replace, or perform corrective work on district technologies or data is also considered vandalism.

- Any such act by a student will be subject to CVES disciplinary procedures as set forth in the CVES Code of Conduct.
- Any such act by staff or guests will be subject to CVES disciplinary procedures as determined by the District Superintendent, including legal action if deemed appropriate.

Damage to CVES technology hardware, software, operating systems, or data due to accident, vandalism, abuse, neglect, or loss by any individual, may result in the individual being held responsible for replacement and/or repair costs.

Users are prohibited from taking data, technology equipment, software or supplies (paper, toner, disks, etc.) out of the building without prior division written consent, or for their own personal use.

- Any such taking or use by a student will be treated as theft and will be subject to CVES disciplinary procedures as set forth in the CVES Code of Conduct.
- Any such taking or use by staff or guests will be treated as theft and will be subject to CVES disciplinary procedures as determined by the District Superintendent including legal action if deemed appropriate.

### **Internet Filtering**

CVES employs firewall, Internet content filtering, and other technologies to secure CVES networks from, and provide safe access to, the Internet and other technology resources, and to comply with federal, State, or local laws or regulations.

CVES may filter or block network traffic or Internet content that disrupts the educational environment or process, or is deemed in violation of, or inappropriate in accordance with the CVES AUP, CVES Code of Conduct, or any other CVES policy or rule, or any federal, State, or local law or regulation.

CVES may filter or block network traffic or Internet content that exposes CVES networks or other technologies to undue risk, or disrupts, degrades, disables, damages or otherwise interferes with normal or efficient operation of CVES networks or other technologies.

Staff, students, parents, guardians, and guests must be aware that content filtering tools are not completely fail-safe, and that while at CVES direct supervision by staff of each student using a computer is desired but not always possible. Users are warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, profane, sexually oriented or potentially offensive to some people. While the intent is to make Internet access available to further educational goals and objectives, users may find ways to access these other materials as well. CVES does not condone or permit the use of this material and uses content filtering software to protect users to the greatest extent possible. Students, staff, and guests are expected to use technology resources in a manner consistent with the CVES AUP and the CVES Code of Conduct, and will be held responsible for their misuse. If a user mistakenly accesses inappropriate information, they should immediately notify the supervising adult or the CVES Technology Department and back out of the site.

### **Privacy and Security**

All staff who have access to or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance

Portability and Accountability Act (HIPAA), and other applicable laws and regulations as they relate to the release of personal information.

CVES students, staff, and guests shall have no expectations of privacy with respect to CVES technology resource usage while on CVES property or while using CVES technology resources. CVES neither intends nor guarantees that data or information created, stored or sent on CVES information technology or network is private. CVES reserves the right to access and view any data or material stored on CVES equipment or used in conjunction with CVES information technology or network. CVES further reserves the right to monitor all computer, network, and Internet activity including transmission and receipt of e-mail, transmission and receipt of files, or any other data that is transmitted, received, or passed through CVES computer systems. This monitoring is for the purpose of computer virus blocking, general filtering of unsolicited bulk e-mail (SPAM), enforcing copyright statutes, and compliance with the provisions set forth in, and required by CVES policies, the Children's Internet Protection Act (CIPA), the CVES Acceptable Use Policy, and all other applicable federal, State, and local laws or regulations.

Users of the CVES computer systems should be sensitive to the inherent limitations of shared network resources. No computer security system can absolutely prevent unauthorized but determined persons from accessing stored information. While CVES has no interest in reading or monitoring the content of electronic communications, it cannot guarantee the privacy or confidentiality of these communications. CVES is required to maintain some material (including all e-mails) that are received by or pass through CVES over varying lengths of time. Public disclosure of certain materials may be required, and CVES must release any such materials, regardless of their content, if required to do so. Therefore, good judgment dictates that an individual using the CVES network or other technologies should create only electronic communications that would not be embarrassing if they became available to the public, or contain any personal information as defined in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and other applicable laws and regulations.

In connection with its responsibilities, the CVES Technology Department may on occasion need to access or monitor parts of the system. All CVES Technology Department members will respect the privacy of personal communications encountered on the systems. However, if CVES Technology Department members, while involved in their routine duties, encounter information that indicates a violation of the CVES AUP, any other CVES policy, or any federal, State, or local law or regulation, they are required to report the existence and source of this information to the proper CVES administrator, and who investigate the matter.

To ensure effective and appropriate use of and access to technology resources, and to enforce technology use rules, the CVES Technology Department may delete files, review accounts, and require users to decrypt any encrypted materials contained in any CVES computer system.

### **Reliability and Limitation of Liability**

CVES makes no warranties of any kind, expressed or implied, for the technology resources it provides to students, staff or guests. CVES will not be responsible for any damages suffered by a user, including those arising from non-deliveries, misdeliveries, service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the user's own risk. CVES specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. Staff, guests, and students (and their parents/guardians) will indemnify and hold CVES harmless from any losses sustained as the result of misuse of CVES technology resources or personal electronic devices by staff, students or guests.

## **Definitions**

**21st Century Skills** - Skills and habits that allow people to participate actively in society using all forms of media available.

**Adaptive/Assistive Equipment** - Adaptive/Assistive equipment includes devices that are used to assist with completing activities for daily living or acquisition of life skills.

**Bandwidth** - Refers to consumed bandwidth, or the average rate of data transfer through a network connection. All users at CVES share a finite amount of bandwidth or capacity of the Internet connection. Activities such as streaming audio and video, and online gaming require large amounts of bandwidth, and degrade overall network speed for others.

**Browsing (or Surfing)** - Viewing Internet content, or using Internet search engines or other resources to find and gather information.

**Cheating** - Use of fraudulent means to complete an academic assignment or test.

Examples of cheating include but are not limited to:

- Looking at notes during a test on information you were expected to learn.
- Looking at and copying answers from your neighbor's paper during a test.
- Texting, messaging, or emailing test or homework answers to a friend.
- Copying an assignment from a friend when you were expected to do your own work.
- Turning in an assignment (test or paper) written wholly or partly for another course for which academic credit was received, without permission.

**Cloud Computing** - Applications, services and storage offered over the Internet, such as Apple's Mobile Me, Mozy backup service, DropBox, and others.

**Communication Systems** - Technologies that include e-mail, web sites, cell phones, IP telephony, analog and digital telephone systems, pagers, text messaging, instant messaging, blogging, podcasting, listservs, and/or other emerging technologies used for communicating.

**Creative Commons Licenses** - Special types of copyright laws that grant owner the right to distribute the copyrighted work worldwide, without changes, at no charge. The details of each of these licenses depends on the version, and comprises a selection of four conditions:

- **Attribution** - Licensees may copy, distribute, display and perform the work and make derivative works based on it only if they give the author or licensor the credits in the manner specified by these.
- **Non-commercial** - Licensees may copy, distribute, display, and perform the work and make derivative works based on it only for noncommercial purposes.
- **Non-derivative** - Licensees may copy, distribute, display and perform only verbatim copies of the work, not derivative works based on it.
- **Share-alike** - Licensees may distribute derivative works only under a license identical to the license that governs the original work.

**CVES Property** - Includes the general campus physical facilities, such as buildings, individual offices, laboratories, desks, file cabinets, lockers, office supplies, furniture and machines, vehicles, and the like. It also means CVES information and communications, including but not limited to all CVES business and educational records, student records, and records of academic and administrative meetings and proceedings whether oral, written or electronic, including records, e-mail, or computer files, and any other information residing on CVES computer systems.

**Cyberbullying** - Includes bullying through email, instant messaging, chat room exchanges, web site posts, or digital messages or images sent to an individual's computer, laptop, cellular phone or personal digital assistant (PDA). Cyberbullying usually involves deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others.

**E-Mail** - Electronic mail. Mail that is composed, delivered and read in an electronic format. CVES provides e-mail services to its teachers and staff. Students and guests are generally not provided e-mail accounts, except on a case-by-case basis when it is part of an approved program or curriculum, and authorized by the CVES technology department and division director responsible for that guest or student.

**Educational Purpose** - Classroom activity, research, career development, and other high-quality, self-discovery activities.

**External/Portable storage or Data-Transfer Device** - A device used to store electronic data that is easily removed or unplugged from a computer so that it may be transported or used with another computer to access the data stored on it.

**Forum / Blog / Wiki** - Any public or private web site or service designed to allow multiple users to publish content or commentary on any subject.

**Guest** - The term 'guest' as used in this document includes anyone not employed either temporarily or permanently by CVES directly, but specifically authorized by a division director or the District Superintendent or designated representative. This includes, but is not limited to, grant-funded programs, outside contractors, and other visitors requiring access to CVES technology resources.

**Hacking** - Attempting to circumvent control or security protocols of a computer system, or attempting to destabilize or deny service to a computer system, or attempting to destabilize or deny service or gain unauthorized access to any part of CVES technology or any other system, internal or external, including, but not limited to computers, printers, network devices, or any other electronic device or means used to provide services to users at CVES.

**Instant Messaging (IM)/Texting/Chat** - The ability to easily see whether a chosen friend or co-worker is connected to the Internet and, if they are, to exchange messages with them. These services include but are not limited to AIM, ICQ, Yahoo Messenger, and MSN messenger, or any application, program, Web site, or part of a Web site that allows text or voice messaging, SMS messaging, paging services, video chat, access to a chat room, real-time chat, Internet relay chat (IRC), or file sharing. This includes services that have a web interface, allowing it to be used on any computer without the need to install software.

**Instructional Day / School Day** - The period of time between the earliest time students are scheduled to arrive and the latest time students are scheduled to depart, and any other time in which instruction occurs.

**Internet** - A vast collection of worldwide computer systems, interconnected for the purpose of sharing and disseminating information.

**Internet Access** - The use of any service provided on the Internet. This includes, but is not limited to: World Wide Web (web or www), electronic mail (e-mail), File Transfer Protocol (FTP), remote terminal (TELNET), chat rooms, Usenet newsgroups, etc.

**Internet Forum / Message Board** - is an online discussion site where people can hold conversations in the form of posted messages. They differ from chat rooms in that messages are typically not available for real-time display, are often visible to the general public, and are usually archived so they can be viewed at a later date.

**Internet Safety** - The security of individuals and their personal information when using the Internet. It is important to understand that many crimes can be committed on the Internet, such as cyberbullying, stalking, identity theft, and more.

**Media Sharing** - Includes but is not limited to sending electronic files via e-mail, instant message, text message, peer-to-peer networking (P2P), posting or linking to media on a web site or blog.

**Netiquette** - Actions that are considered proper etiquette while using Internet resources. For example, composing an e-mail message entirely in capital letters is considered shouting and would be considered rude.

**Network** - A collection of computers or other devices connected together to share resources.

**Operating System** - Software, consisting of programs and data, that runs on computers, manages hardware resources, and provides services for running application software. Operating systems are found on many electronic devices including cell phones, video game consoles, laptop and desktop computers and servers.

**Peer-to-Peer File Sharing (P2P)** - Any application, web site, or service that allows users to share files, music, movies, video clips, or any other media over the Internet with, or without having to purchase their own copy. This includes any application, web page or device that can use the Internet to exchange files with each other through a mediating server, or by directly accessing files from another computer.

**Personal Digital Assistant (PDA)** - a mobile device that functions as a personal information manager. A PDA typically includes an appointment calendar, to-do list, address book, calculator, and some sort note taking program. Nearly all smartphones are also PDAs.

**Personal Electronic Device** - Any device that a person is in possession of, which electronically communicates, sends, receives, stores, reproduces or displays voice or text communication or data. These include but are not limited to cellular phones, pagers, smart phones, music and media players, gaming devices, tablets, laptops and personal digital assistants.

**Personal Information** - information about yourself, including but not limited to your address, phone number, student number, date of birth, or social security number, or anything else that is defined in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and other applicable laws and regulations as they relate to the release of personal information.

**Plagiarism** - The use or close imitation of the language and ideas of another author and representation of them as one's own original work. This includes copying from electronic sources (from the World Wide Web), even with minor alterations.

Examples of plagiarism include but are not limited to:

- Copying a passage verbatim from an information source without attributing the source.
- Rephrasing someone else's original idea without giving credit to that person.
- Turning in work that was purchased from an online essay mill or from another student.

**Portable OS / Portable Desktop Environment** - Any program that can be installed on a computer or removable storage device that provides the user with an operating system, application launcher, or virtual computing environment that runs either within, or instead of, the native operating system. Examples would include but are not limited to U3, StartKey, Knoppix (and many other linux variants), virtualbox, etc.

**Print Resources / Digital Documents** - Any written item, such as a book, article, or letter, especially of a factual or informative nature. Digital documents are those same resources, available in electronic form that are readable and manipulable by computer.

**Private Network Resources** - Any electronic device, system, or service owned, operated or licensed by CVES, that is accessible from a computer or other electronic device which is not available to the general public. Examples include but are not limited to network printers, file servers, application servers, communications servers, network storage, network ports, student information systems, databases, etc.

**Public Domain** - Ideas, information, and works that are "publicly available", and are not covered by intellectual property rights at all (i.e. copyright, patents, and trademarks, etc.), if the intellectual property rights have expired, or if the intellectual property rights are forfeited, and information which is intangible to private ownership.

**Remote Access / Administration / Monitoring** - Refers to any method of accessing, controlling or logging into a computer, or viewing the contents or screen from a remote location.

**Social Networking Site** - Any website or service that allows users to create a "profile" describing themselves and to exchange public or private messages and has the ability to list or share other users or groups to which they are connected.

**System and Software Updates / Patches**— A piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.

**Spam** - Unsolicited e-mail, usually of a commercial nature and usually sent to multiple recipients. Spamming also includes sending a high volume of annoying or bothersome messages to the same recipient(s), including mass mailings to individual CVES staff, or internal mailing lists.

**Staff** - The term 'staff' as used in this document includes all permanent and temporary personnel hired by CVES.

**Student** - The term 'student' as used in this document includes any person enrolled in any class or educational program at CVES.

**Teacher** - The term 'teacher' as used in this document includes any staff responsible for delivering curriculum to students, providing direct instruction to students, or responsible for direct supervision or care of students.

**Technology Resources** - Includes any and all computer and network resources. This includes both software programs, hardware, assistive or adaptive equipment and peripherals such as printers, modems, as well as, fax machines, copiers, Internet access, e-mail, documents, etc.

**Virus Protection Software Package** - An application or software suite used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware and adware.

**Visiting School District Laptops And Electronic Devices** - Any laptop or electronic device owned by any school district that has in place a Board approved Acceptable Use Policy and Code of Conduct. These devices and laptops present a reduced risk to CVES network or technologies because they are owned and maintained by a school district, are typically compatible with CVES technologies, and are kept to similar standards as CVES technologies in regard to security, virus protection, applications, and operating systems.

*\* The owner and all users of such laptops or electronic devices must have a signed Acceptable Use Policy agreement on file with their home district.*

**Visiting School District Personnel** - Any guest employed or enrolled in any school district or BOCES that has in place a Board approved Acceptable Use Policy and Code of Conduct, who has a signed agreement to that policy on file with the home district.

**Web 2.0** - Sites that allow users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to web sites where users are limited to the passive viewing of content that was created for them. Examples of Web 2.0 include social networking sites, blogs, wikis, etc.

**Web Cam** - A video camera whose current or latest image is broadcast from a web site or application. A live cam is one that is continually providing new images that are transmitted in rapid succession or, in some cases, in streaming video.

**Webinar** - A workshop or lecture delivered over the Web. Webinars may be a one-way Webcast, or there may be interaction between the audience and the presenters.