Legal Review: 02/2024
Adopted: 06/17/98
Reviewed: 03/17/04, 05/20/20
Revised: 01/16/02, 06/16/06, 06/20/07, 06/27/12, 03/18/15, 01/17/18, 04/18/22, 03/20/24

Computer Usage and Internet Safety

The Chenango Valley Board of Education believes that technology is a fundamental tool whereby students can learn to obtain information, solve problems and communicate. Access to this technology should be available to all, enabling each student to become a lifelong learner and productive member of our global society.

The Professional Development Team will work closely with the Superintendent or his/her designee to coordinate in-service programs for the training and development of District staff in computer skills and the incorporation of computer use in the curriculum. Use of the computer network as an integral part of the curriculum will be encouraged. Through software applications, online databases and electronic mail, the network will significantly enhance educational experiences and provide statewide, national and global communications opportunities for faculty, staff and students.

A staff account will be established for each user who requests access to the District's computer system only after completing the attached form. This account will be nontransferable and be used only in the support of education and research. This account may include access to electronic mail, online services, web-based platforms, software licensed to the District, and the Internet. It may also include the opportunity for staff to have remote access to the District Computer System ("DCS") from their home or other remote locations, and/or to access the DCS from their personal electronic devices. All use of the DCS and the wireless network, including remote use off of school premises and use on personal electronic devices, will be subject to this policy and any accompanying regulations.

With access to computers and people all over the world also comes the availability of some materials that may not be considered to be of educational value within the content of the school setting. The District has taken available precautions, including the use of filtering software, to restrict access to inappropriate content. While this filtering software is being constantly updated, no technology tool can take the place of appropriate supervision of student online activities by responsible adults. On a global network, it is impossible to have total control over access to inappropriate content, and it is possible that, despite the District's best efforts, an industrious user may discover it.

The District firmly believes that the valuable information and interaction available on this network far outweigh the possibilities that users may procure material that is not consistent with the educational goals of this District. It shall be the responsibility of all members of the District's faculty and staff to supervise and monitor access to the Internet in accordance with this policy and the Children's Internet Protection Act. Furthermore, students will receive education about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyber bullying awareness and response.

Chenango Valley Central School District Computer Use Guidelines

The smooth operation of the District Computer System ("DCS") relies upon the proper conduct of the end users who must adhere to strict guidelines. The following guidelines are provided so that users are aware of their responsibilities. If a Chenango Valley Central School District ("CVCSD" or the "District") user violates any of these provisions, his or her account may be terminated and future access could be denied.

The Superintendent and administrative staff will be responsible for governing the use, supervision and security of the District's network in compliance with the following Computer Use Guidelines:

1. **Acceptable Use:** Any use of your account must be in support of education and/or academic research, and must be consistent with the educational objectives of CVCSD. Unauthorized access, including "hacking" and other unlawful activities are strictly prohibited. Transmission of any materials in violation of any federal or state law is also prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, material which promotes violence or hatred against particular individuals or groups of individuals, material which advocates the destruction of property, or material protected by trade secret. Use for commercial activities by non-profit institutions is generally not acceptable. Use for product advertisement is also prohibited.

   District faculty and staff are further prohibited from using software, applications or other technologies pursuant to a click-wrap agreement in which a third-party contractor receives student data or teacher or principal data from the District, unless they have received prior approval from the District's Data Privacy Officer or designee.

2. **Privileges:** Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or his/her designee. They will determine what appropriate use is, take appropriate action and determine consequences, including, but not limited to, revoking a user's account. The administration, faculty, and staff of CVCSD may request the system administrator to deny, revoke, or suspend specific user accounts.

3. **Student Personally Identifiable Information (PII) Data Access:** All access and use of student PII data will be done in accordance with a user's direct job responsibilities. Confidentiality and laws governing student privacy such as [FERPA, IDEA and NYS Education Law § 2-d] must be followed. Users will protect the privacy of PII by:
   a) Ensuring that every use and disclosure of PII by the User benefits students and the District by considering, among other criteria, whether the use and/or disclosure will:
      1. Improve academic achievement;
      2. Empower parents/guardians and students with information; and/or
      3. Advance efficient and effective school operations.
   b) Not including PII in public reports or other public documents.

4. **Social Media Usage:** The Board of Education respects the legal rights of employees, including the protection of union employee activities under the New York Public Employees' Fair Employment Act (a.k.a. the "Taylor Law"). The Board also recognizes an employee's right to free speech and the desire of employees to speak out on issues of public concern. However, CVCSD expects and trusts its employees to exercise professionalism and personal responsibility whenever they use social media, which includes adhering to all policies, rules and regulations governing employee conduct set by the Board and the CVCSD administration, and ensuring that the legitimate business interests of the District are not compromised.

5. **Definitions:**
    a) "Social media" includes but is not limited to all means of communicating or posting of information on the Internet and/or mobile telephone networks. Examples of social media include, but are not limited to Facebook, X (formerly known as Twitter), YouTube, Instagram, Snapchat etc. Social media also includes an employee's own or someone else's web log, blog, online journal, personal website, online bulletin boards, chat rooms, content sharing services, podcasts, and other, similar methods of disseminating information over the Internet and/or mobile telephone networks.
    b) "Employee" includes any person employed by the Chenango Valley Central School District.

6. **Employee Certification:** Employees are solely responsible for what they post, and, by their acknowledgement of receipt of this policy, Employees certify that they are aware of the following:
    a) Online conduct can potentially adversely affect their job performance, the performance of other employees, relationships with parents/guardians/students and the District.
    b) Even when posting to social media as a private citizen, content posted by employees may adversely impact the District and/or its employees and students. Accordingly, posts as private citizens may subject an employee to discipline action related to their position with the District.
    c) The District may observe content and information made available by an employee on the Internet including content posted outside the workplace or workday.
    d) DCS users should have no expectation of privacy with respect to any e-mail records, images, files or other data they store on District servers. DCS administrators may review stored files and communications at any time, without notice. If any data stored on District servers is found to be in violation of this policy, any other applicable District policy, rule or regulation, or any federal, state or local law, disciplinary action may be taken against the responsible user, up to and including reporting the user to appropriate law enforcement agencies.
    e) Employees must ensure social media posting is consistent with existing district policies, including FERPA and all other data privacy laws and regulations that apply to specific departments and funded programs.
    f) Personal/private social media account names or email names shall not be tied to the district when posting.
    g) District logos and badges must not be displayed in any post to social media that promotes an employee's private businesses or is intended for personal, pecuniary gain.

7. **Network Etiquette:** DCS users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
   a) The use of abusive or objectionable language in either public or private messages is not permissible. Do not swear or use profanity. Electronic bullying or harassment will not be tolerated.
   b) Do not use the network in such a way that it could disrupt the use of the network by others. This includes sending "chain letters", "broadcast" messages, and "junk mail" to lists or individuals and any message that is likely to result in the loss of a recipient's work or systems.
   c) Do not access, upload, download or distribute pornographic, obscene, or sexually explicit material.
   d) Do not share your password with others or use anyone else's login information.

8. **Disclaimer of Responsibility:** CVCSD shall not be responsible for any damages that a user may suffer as a result of his/her use of the DCS. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by user negligence, errors or omissions. Use of any information obtained via the Internet is at your own risk. CVCSD denies and hereby disclaims any responsibility for the accuracy or quality of information obtained.

9. **Cybersecurity:** Security on any computer system is a high priority. If you detect a potential cybersecurity issue, or you are the victim of a "phishing" scam while using DCS, please notify the Superintendent or his/her designee immediately. Do not use another individual's account, forge messages or post anonymous messages. Any attempt to log in to the DCS with account credentials of another user, or as a system administrator may result in the cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the DCS. Users will not install any software or download any files (e.g., MP3's) to the District's network unless authorized by the technology department. Always log-off when you leave a computer, as all activity involving your account is your responsibility.

10. **Vandalism/Theft/Damage to DCS:** Any form of willful vandalism to, or theft of DCS hardware, software, programs, files or student PII will result in cancellation of user privileges. This includes, but is not limited to, contamination, deletion, or reconfiguration of data or degradation of system performance in any way.

11. **Plagiarism:** Plagiarism is taking ideas and/or words of someone else and appropriating them as your own. Rules for properly crediting research sources apply for the Internet and other online computer networks. Plagiarizing the work of another may result in the cancellation of user privileges.

Chenango Valley Central School District
Computer Usage Sign-off

FACULTY OR STAFF

I have read the Computer Usage and Internet Safety Policy and I understand and will abide by the Computer Use Guidelines. Should I commit any violation, I further understand that my access privileges may be revoked. I further understand that any violation of the regulations above may be unethical, may constitute a criminal offense, and may result in legal and/or disciplinary action against me.

Name (print clearly): _____

Signature: _____ Date: _____

Building: _____

Title: _____

Office Use:

Email Lists Needed: _____

SchoolTool Group(s): _____

Device Needed: _____

Other Notes: _____

_____