Acceptable Use Policy - Computer and Network/Internet Guidelines and Conditions of Use

Computer and network access, including Internet access, is available to students and staff of the District. CMS is a Children's Internet Protection Act (CIPA) compliant School District and therefore is required to use a content filtering system to regulate access to and from Internet sites. Please read this document carefully. Our goal in offering these services to our school community is to promote educational excellence in schools by providing resource sharing, innovation, and communication.

Technology offers the potential of access to such services as:

- Computer-based tools and applications
- Instructional resources and materials
- Networked references, research sources, and library catalogs
- Electronic mail services
- Global information and news
- Correspondence with other institutions
- Online publishing and information sharing

With access to computers and people all over the world also comes the availability of material that may not be considered educationally valuable in the context of the school setting. However, on a global network it is impossible to control access to all materials, and an industrious user may discover controversial information. CMS firmly believes that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may acquire material inconsistent with the educational goals of the District. The smooth operation of the network relies upon the proper conduct of the end users who must strictly adhere to the following guidelines and conditions of use. These guidelines are provided so that users are aware of the responsibilities they are about to acquire. In general, this requires ethical and legal utilization of the computer and network resources.

This Acceptable Use Policy is binding on all users of the CMS school community site as a matter of law, whether this agreement is signed or not. The guidelines and conditions outlined in this policy in no way limit the school districts prerogative to manage its technology systems as it sees fit, or restrict its authority to take any actions it deems necessary to adequately supervise, protect, and if necessary, discipline students and staff. CMS reserves the right to revise this policy at any time, and all revisions will take effect immediately, upon approval by the CMS administrators.

Acceptable Use

The purpose of educational technology in CMS is to support its educational goals. Your use of technology must be consistent with the educational objectives of CMS. Use of computer systems and networks imposes certain responsibilities and obligations on users and is subject to CMS policies and local, state, and federal laws. Acceptable use must always be ethical, reflect honesty, and show courtesy in the utilization of shared resources. It demonstrates respect for intellectual property, ownership of information and system security mechanisms.

Privileges/Consequences

The use of technology is a privilege, not a right, and inappropriate use may result in restriction of privileges and other disciplinary action. Listed below are examples of user activities that CMS deems inappropriate and in violation of this policy. CMS reserves the right to expand this list as necessary. CMS retains the right to deny, revoke, or suspend specific user privileges or restrict access to technology resources, require payment for any damage, and bring criminal charges if deemed necessary. Any material used, generated, received, or stored by any user through the use of CMS computers, networks or other technology is subject to review. The CMS Technology Department has been given the responsibility of monitoring all network activities. CMS reserves the right to examine, restrict, or remove any material that is on or passes through its technology systems. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form. Parents, or legal guardians, may request to see the content of any material created or accessed by their child/children, if technically possible.

Examples of user activities that violate this policy:

- Commercial advertising or unethical/illegal solicitation
- Accessing a file or web site that contains pornographic or obscene pictures, videos, stories, or other material; making copies of such material, or distributing or exposing others to such material
- Using copyrighted material without permission when such is required
- Sending or receiving messages that are obscene, profane, racist, sexist, inflammatory, threatening, disruptive, violent, or slanderous toward others
- Creating, distributing, and/or placing a computer virus on the network or any workstation
- Sending messages or information with someone else's name on it or misrepresenting the source of information you enter or send
- Harassing others or requesting or distributing addresses, home phone numbers, or other personal information
- Cyber-Bullying
- Sending chain letters or engaging in "spamming" (sending an annoying or unnecessary message to large numbers of people).
- Purchasing goods and/or services, which obligates CMS to another party.
- Revealing home addresses, e-mail addresses, or phone numbers of other students or colleagues.
- Sharing passwords. The only person to ever use a password is the authorized person to whom it has been issued by CMS.
- Attempting to access and/or alter information in restricted areas of any network or in any way violate the confidentiality rights of other users on any network.
- Failing to report violations of this policy or other conditions that may interfere with the appropriate and efficient use of school resources. Users are required to report any of the following to his/her teacher, supervisor or the building network administrator as soon as the following are discovered:
- Any messages, files, Web sites, or user activities that contain materials that are in violation of this policy.
- Any messages, files, Web sites or user activities that solicit personal information about you or someone else, or request a personal contact with you or another user (i.e. asks for

your address, phone number, photograph, email address, or other personal information for any network site, credit card number, Social Security number, or to meet you.)
- Attempts by any user to abuse or damage the system; violate the security of the network and its resources; obtains access to secure, restricted or confidential information without authority from CMS; hacking.
- Any illegal activity or violation of school policy.
- Political Lobbying
- Fundraisers
- Chat Rooms
- Instant Messaging Sites
- Streaming Audio (listening to the radio over the network)
- Streaming Video (watching full length movies, etc. over the network)
- Do not allow ANY non-CMS employee to "work on", "fix", use or download unauthorized programs or features on School District computers (desktop, laptop or mobile device)

Security

Security on any computer system is a high priority, especially when the system involves many users. Any user identified as a security risk or having a history of problems with other computer systems may be subject to severe restriction or cancellation of privileges. CMS reserves the right to examine, restrict and/or remove any material that is on or passes through its technology systems. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

If you feel you have identified a security problem on the network:
- You must notify the Chief Technology Officer or Coordinator of Technology, as well as your immediate supervisor.
- Do not demonstrate the problem to other users

Security violations are:

1. Attempts to log on to any network, as a system administrator
2. Attempts to compromise the security, integrity, and functionality of any CMS technology system
3. Possession of tools, which are designed to do so, while on school property
4. Uploading or creation of computer viruses
5. Deletion or alteration of other user's files
6. Loading of applications removing protection from restricted areas
7. Unauthorized blocking of access to:
    - Information
    - Applications
    - Areas of the network
8. Introduce or attach any software or hardware to technology used in CMS, which is not authorized by the Chief Technology Officer or Coordinator of Technology
9. Modification to any hardware or software owned or managed by CMS, which is not authorized by the Chief Technology Officer or Coordinator of Technology

Network Etiquette
The user is expected to abide by the generally accepted rules of network etiquette. (NEPN/NSBA Code: IJNDB – E2)

1. Users shall be polite in all communications.
2. Use appropriate language; swearing and vulgar language are considered inappropriate.
3. Do not reveal home addresses, e-mail addresses, or phone numbers of other students or colleagues.
4. Electronic mail (e-mail) is not guaranteed to be private. CMS scans all email for viruses, malware, adware, spyware, spam and content.
5. Do not use network in any way that would disrupt its use by other users.
6. Messages relating to, or in support of, illegal activities may be reported to the authorities.
7. Consider that communications and information belonging to other people should be treated as private property.

Web Publishing
CMS Web site (www.clovis-schools.org) is maintained by the District Webmaster. In order to maintain consistency of layout, only the webmaster is authorized to implement any change to the Web site.

Content Changes

1. Employees and students may make changes to content of a site established or maintained by the employee or student on the CMS network, with authority from CMS.
2. Changes are submitted to the site's administrator and/or Superintendent's designee for approval.
3. Approved changes are submitted to Webmaster, who will change the Web site.

Layout Changes

1. Site administrators may request layout changes for their Web site.
2. Changes are submitted to the Chief Technology Officer for review.
3. Approved reviews are submitted to Superintendent's designee for approval.
4. Approved changes are submitted to Webmaster, who will change the Web site.

Employee Sign-Out Form & User Agreement for CMS Technology Equipment

- CMS Staff Members may be issued, assigned and authorized to utilize CMS technology equipment for business, instructional, or school-related purposes ONLY, including: laptops, tablet computers, scanners, cameras, Kindles, Smart-pens and Projectors.

- At the time such equipment is issued and assigned to the Staff Member by CMS, the employee will be required to fill out and sign the "Employee Sign-out Form and User Agreement" for such technology equipment.
- All equipment assigned to you will be on loan for a period specified in the Form, but in no event later than the last day of your employment with CMS, or upon return of the equipment to the CMS IT Department in good and working condition.

- You are bound to follow all CMS technology guidelines and Acceptable Use policies when using CMS electronic equipment.

- All equipment issued to you by CMS must be returned in good and working condition at the end of the assigned period or on or before your last day of employment with CMS, whichever is earlier, NO EXCEPTIONS.

- Upon return, equipment will be inspected by IT Staff to ensure it is still in good and workable condition, as it was when assigned to you, normal wear and tear is excepted.

- Should the equipment be lost, damaged or destroyed, or should you fail to return the equipment assigned to you, as well as its corresponding parts (i.e. charger, batteries, etc…), on or before the end of the assignment period or the last day of your employment with CMS, whichever is earlier, you will be responsible for paying or reimbursing CMS for the cost of repair or replacement of the equipment.

- Payment for repair or replacement of equipment will be due no later than thirty days after the IT Department give you notice of the repair or replacement cost, or on the last day of your employment with CMS, whichever is earlier.

- Should you fail to pay for or reimburse CMS for the repair or replacement cost of the equipment, CMS is hereby authorized to deduct such costs from your payroll following reasonable notice to you.

Warranty
CMS makes no warranties of any kind, whether expressed or implied, for the service it is providing. CMS will not be responsible for any damages users suffer. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at the user's risk. CMS specifically denies any responsibility for the accuracy or quality of information obtained through its service.