Caledonia Community Schools
High School Acceptable Use Policy

This acceptable use policy applies to all users accessing the network, the Internet and equipment at Caledonia Community Schools, both on-site and remote connections.

Use of all technology at Caledonia Community Schools is a *privilege* extended to students. Our goal in providing this service is to promote an educational excellence in a safe environment by facilitating resource sharing, information gathering skills, diversity, personal growth in technology, innovation, and communication.

Network/Hardware Use - Users are to handle all technology equipment with proper care and respect and in the manner intended. Users may save files to the network, however, any files stored under user's ID or on any media by the user or Caledonia Community Schools are under supervision of the Network Administration. User will not encrypt any files stored on the network, or override system files. All files stored on school accounts, hard drive, or portable media may be viewed, modified, or deleted by any designated Caledonia Community Schools staff member at any time. Users will only access the network or internet on hardware authorized by the Network Administrator or his/her representative.

User Accountability - Users are held responsible for all material sent and received under their account. User will not attempt to "hack", to gain unauthorized access, (ie: using web proxy services to bypass firewall) or attempt other unlawful activities on any CCS servers. Users are required to sign an Acceptable Use Policy in order to use the school network. Parent permission is necessary for students to access the Internet.

Passwords and User names - A user identifier known as a user name and password are required of all users. Passwords **must not** be shared with any other user FOR ANY REASON! The password must be changed as soon as possible after an unacceptable exposure or suspected tampering by another user. User **will not give** others permission to use their ID or password.

Unauthorized Access - Users will not represent themselves as another user, attempt to receive messages or access information, or copy, or modify files or data that does not belong to them.

Notification - Users must notify their building's computer technician immediately when they become aware that another student has gained access to their personal account.

Internet Access - User will use e-mail only when it pertains to course work and is necessary to complete a course assignment. Students may NOT use the email for non-educational purposes. User may be asked to explain an e-mail that may not appear to be educational. User will not send hate mail, harassment, discriminatory remarks or use other antisocial behaviors on the Internet. User will not send any mail as an anonymous unsigned message. User will not reveal any personal, confidential or private information about themselves or other individuals, such as home addresses, phone numbers, etc. User will not access chat room unless authorized.

User will not order or make a commitment to pay for any goods or services via Internet. User will report any violations of the use of the Internet to the Internet administrator.

Student will not access, download, save or print any inappropriate information in words, pictures, movies, sound files, cartoons, or other.

Students are NOT allowed to use the school network, hardware or internet to play games of any kind at school. Gaming devices such as PS2 or like devices will not be permitted in the building.

Students are NOT allowed to download or install movie trailers, games, or other similar applications using the school network.

Software Use - All software used on CCS computers must be appropriately acquired and used according to the appropriate licensing. Possession or use of illegally copied software is prohibited. Likewise, users shall not load, copy, install, delete or tamper with any files or application programs owned by Caledonia Community Schools or not owned or created by user without prior approval.

File Use - User will save all personal, non-educational files on their own portable media. User will not access, save or download inappropriate files or files known to carry harmful viruses via the school network.

Printer Use - User will not abuse printer server rights by purposely sending to the printer or printer queue blank pages, documents that are very long in length (i.e. more than 8 pages), documents containing profanity, abusive language, or threats, documents for personal use (i.e. notes to friends), or any unrecognized command causing fatal errors to the printer or printer queue.

Malicious Software - Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms. User will not intentionally tamper with the system software, or violate copyrights and licenses on applications, files, icons or sound files.

Disciplinary Actions for Violation of Policy - The guidelines on the preceding pages are not all-inclusive, but only representative and illustrative. A user who commits an act or misconduct which is not listed may also be subject to disciplinary action.

Disciplinary actions are based on the discipline procedures of Caledonia Community Schools. Staff intervention strategies such as teacher/student conferences, auxiliary staff/student intervention and teacher/ parent contacts may be used for acceptable use policy violations. Any or all of the following intervention strategies and disciplinary actions may be used by administrators.

Actions as deemed appropriate may include:
Administrator/student/parent conference or reprimand.
Suspension from accessing the Internet, network, or using any technology hardware.
Expulsion from school.
Confiscation of inappropriate item(s).
Full financial restitution to Caledonia Community Schools which includes time and materials.
In or out-of-school suspension.
Behavioral contract.

Non student users are also responsible for abiding by all the policies and procedures set forth in this document. Failure to do so may result in the loss of user privileges and disciplinary action. Repeat violations may warrant permanent removal of privileges.

In accordance with Board Policy #7540 – modified 6/17 md