Coopersville Area Public Schools
Middle School/High School Student LAN, Network/Internet Acceptable Use Agreement and Technology Code of Ethics

The State requires all districts to have an Acceptable Use Policy and receive assurances that students will abide by said policy.

Coopersville Area Public Schools (CAPS) provides students with access to the District's electronic local area network (LAN) which includes Internet access (Network/Internet). The purpose of the LAN is to enhance learning. CAPS seeks to improve the computer literacy of its students and assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information.

The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

Access to the LAN is a privilege that may be revoked by the District at any time and for any reason. CAPS seeks to protect legitimate computer users by imposing sanctions on those who abuse this privilege. Unacceptable behavior may lead to additional penalties such as other disciplinary action and/or legal action. The staff of Coopersville Area Public Schools will be the sole arbiter of what constitutes unacceptable use of behavior as outlined by this document which may be changed without notice.

If a student suspects or identifies a security problem in the school's computers, network or Internet, that student shall promptly notify a system administrator or teacher. To avoid any damage, the student shall not in any way demonstrate the problem to others. The student should not go looking for security problems, because this may be construed as an illegal attempt to gain access.

The LAN and all associated computer hardware, software, data and files are the property of CAPS. CAPS LAN is a monitored network. Authorized school personnel may read all files and messages of any user. Therefore, students should expect no privacy in the contents of personal files on the District system. Parents may have the right at any time to request to see the contents of a student's electronic files.

CAPS will cooperate fully with local, state or federal officials in any investigation related to any illegal activities conducted through the LAN/Internet.

CAPS makes no guarantee that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system.

Students will utilize the computer hardware with care. Items such as food, drink and candy shall be kept completely away from any computer hardware. Students will not physically abuse/move any hardware (case, keyboard, mouse, monitor, etc.) or computer furniture. Students will not make any hardware changes (move mice or mouse balls, keyboards, cords, etc.). Students will not change any computer settings without permission (wallpaper, desktop etc.).

The primary purpose of the CAPS LAN is educational and, as such, shall take precedence over all other purposes. The CAPS LAN and its resources are intended for the private use of its registered users. Any use of these resources for commercial for profit or other unauthorized purposes (i.e. advertisements, political lobbying), in any form is expressly prohibited.

A. Appropriate reasons for revoking privileges include but are not limited to:
    1. The altering of system software.
    2. Connecting any type of external device to the LAN or to district computers, whether connected to the LAN or not, without specific written permission of the Technology Department.
    3. Storing inappropriate information, graphics, or data on computers and/or servers in either public or private file storage locations.

4. Engaging in illegal acts and malicious behavior, such as threatening the safety of a person, harassing, insulting or attacking others, engaging in criminal activity, use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, defamatory or discriminatory remarks, sending or displaying offensive messages or pictures, obtaining copies of or modifying files or data belonging to other users, etc.
5. Engaging in electronic cheating of any form using any electronic device, such as creating files with answers to tests or quizzes, sharing files with assignments for other students' use, using PDAs to beam answers, etc…
6. Transfer of material that may be considered treasonous or subversive via the District's Internet.
7. Use of any e-mail, chat, instant messaging or unauthorized web site communication using network equipment and resources.
8. Accessing or attempting to access restricted network areas or areas beyond the student's authorized access.
9. Collecting or attempting to collect passwords of other network users by either overt or covert methods, allowing anyone to use an account other than the account holder or misrepresenting other users on the network.
10. Deliberate attempts to disrupt the computer system or destroy data by spreading any computer viruses, including student created viruses, or by any other means.
11. Illegal installation of copyrighted software.
12. Unauthorized copying of licensed or copyrighted software.
13. Unauthorized downloading and/or installation of software on client or network computers.
14. Interfering with others' use of the network, including but not limited to disrupting the operation of the network through abuse of hardware or software, intentionally wasting limited resources, physical or electronic tampering with computer resources. Students shall not access, alter or otherwise tamper with the computer's system files, network files or other students' files. Students shall not install, download from the Internet or copy any executable file onto the network or computer workstation unless specifically authorized to do so by the technology coordinator. In addition, students shall not view, access or alter any directory or drive other than the one to which they are assigned.
15. Employing the network for commercial purposes.
16. Creation, storage and/or posting of any web pages except for class requirements
17. Playing computer-based and Internet-based games except those determined by the supervising teacher and/or technology coordinator as having educational value.
18. Any user identified as a security risk or having a history of problems with other computer systems.
19. Students shall not use school resources to engage in "hacking" or attempts to otherwise compromise the security of the CAPS network or any other network.

B. Student Expectations in the Use of the Internet
1. Students will not post personal contact information about themselves or other people. Personal contact information includes address, telephone number, school address, work address, etc.
2. Students agree not to meet with anyone they have met online without their parent's approval. Their parent should accompany them to any such meeting.
3. Students will promptly disclose to their teacher or other school employee any message that they receive that is inappropriate or makes them feel uncomfortable.
4. Students will not plagiarize works from the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own.
5. Students will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, ask.
6. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. CAPS, in association with the Ottawa Area Intermediate School District, has taken appropriate precautions to restrict access to controversial materials. However, on a global network, it is impossible to control all materials and an industrious user may discover controversial information. CAPS firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may access material that is not consistent with the educational goals of the District. CAPS Internet will not

be used to access material that is profane or obscene (pornography), that advocates illegal acts or that advocates violence or discrimination towards other people (hate literature).

7. If a student mistakenly accesses inappropriate information, the student will immediately tell the supervising teacher or other District employee. This will protect the student against a claim of intentionally violating the Acceptable Use Policy.
8. If there are additional material that parents believe would be inappropriate for their child(ren) to access, parents should instruct their child(ren) accordingly. The district fully expects that students will follow their parent's instructions in this matter.

MIDDLE SCHOOL AND HIGH SCHOOL DISCIPLINARY ACTION PLAN

Users violating any of these privileges and responsibilities will face disciplinary action deemed appropriate in keeping with the disciplinary policies and guidelines of the school. Coopersville Area Public Schools is the judge of the seriousness of violations of the acceptable use policy. Disciplinary procedures may be escalated/accelerated based on the seriousness of the violation.

Users in violation may be required to make full financial restitution for investigating and remedying damages caused by unauthorized and/or prohibited actions. The middle school and high school administration reserves the right to administer disciplinary action in a discretionary manner.

High school and middle school students will be disciplined for violating the privileges outlined in the above document. Violations of this network and Internet policy are cumulative for grades 6-8 and again in 9-12.

RECOMMENDED DISCIPLINARY GUIDELINES

Accelerated Discipline: The following guidelines are for minor offenses. Major offenses will result in accelerated discipline which means that one or more steps in the disciplinary process may be skipped. Some offenses may result in immediate loss of all computer privileges and treated as a Fourth Offense. Some offenses may also violate other parts of the school's disciplinary code, and as such, will be treated accordingly (in addition to the steps listed below). Some offenses may also be violations of local, state or federal laws, and as such, will be referred to the proper authorities.

All computer privileges may be suspending during the investigation of any alleged offenses.

First Offense: The student will lose all computer privileges for two (2) weeks. The offense will be recorded in the student's file. The student will review the Acceptable Use Agreement and Technology Code of Ethics with the appropriate staff member before computer privileges will be reinstated.

Second Offense: The student will lose all computer privileges for six (6) weeks. The offense will be recorded in the student's file. The student will be expected to write a technology behavior plan for himself/herself before computer privileges are restored. The student, his/her parents, the District Technology Coordinator and a building administrator will sign this plan.

Third Offense: The student will lose computer privileges for the time equal to one semester. When privileges are reinstated, they will be so on a limited basis.

Fourth Offense: The student will lose computer privileges permanently.

Any intentional violation which affects the integrity of the network may result in permanent removal from the network.

Coopersville Area Public Schools
Student LAN, Network and Internet Services Agreement Form

STUDENT USER SECTION

I have read, understand and will abide by the above Student LAN, Network/Internet Acceptable Use Agreement and Technology Code of Ethics. I further understand that if I violate the rules, my account can be terminated. I may face other disciplinary measures as well as appropriate legal action. By signing below I am acknowledging that I have read the entire agreement and agree to the terms described in this agreement.

Signature of student: _____ Date: _____

Printed name of student: _____

PARENT/GUARDIAN SECTION

As the parent or guardian of this student, I have read the Student LAN, Network/Internet Acceptable Use Agreement and Technology Code of Ethics. I understand that this access is designed for educational purposes only. I recognize that it is impossible for the Coopersville Area Public School District to monitor the quality of all materials obtained through third party sources, and I will not hold them responsible for materials acquired on the network or Internet. I will emphasize to my child the importance of following the rules for personal safety. I have read and understand the information contained in this document and hereby give permission to issue an account for my child and certify that the information contained in this form is correct. I also agree to pay the District for fees, expenses or damages incurred as a result of my child's misuse of the network or equipment. By signing below, I am agreeing to the terms described in this agreement.

Parent/guardian signature: _____ Date: _____

Printed name of parent/guardian: _____ Phone: _____