Clay Community Schools

Terms and Conditions

Use of Corporation-Provided Computer Networks and Internet

1. **Clay Community Schools (CCS) Network and Internet Access** – CCS network access is available to authorized CCS Students, faculty and staff members subject to the Terms and Conditions found in this document. The purpose of the access is to facilitate communications in support of research and education. Students utilizing CCS networks and Internet access must first sign an acceptable use agreement and students wishing to have Internet access must also have the signed permission of a parent or legal guardian. Signatures on the agreements are legally binding and indicate the parties who signed have read the Terms and Conditions set forth in this document as well as the

Acceptable Use Policy (AUP) of Clay Community Schools and understand their significance.

Use of a school-provided account is a privilege, not a right and inappropriate use may result in the cancellation of all network and/or Internet privileges and additional disciplinary action. Parents and guardians have the option of requesting for their children alternative activities not requiring Internet use. Such a request should be submitted to the building principal in writing.

2. Acceptable Use – The intended use of each CCS network and Internet account is to support education and research which is consistent with the educational objectives of Clay Community Schools. The smooth operation of the network relies upon the proper conduct of each end user who must adhere to the guidelines of Clay

Community Schools. A user is responsible for all on-line activities that take place from a school site through his or her account.

The following uses of the CCS networks or Internet access are prohibited:

a. **Program Access:** Students may not access any program or part of a program not assigned by a CCS staff member. Students may not access any e-mail account using CCS computers. School administrators may grant exceptions.

b. **Diskettes:** Students may not copy any program or file to or from a diskette or other media. A CCS staff member may grant exceptions.

c. **User Accounts:** Students may not access another individual's files, information, or software without prior authorization from a CCS Staff member. All users must login using their own user ID, keep all passwords secret and contact a staff member immediately if a password has been learned by another person. Users may not vandalize damage, disable or "hack" the files of others.

d. **System Resources:** Users should not use the network in such a way that would waste system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing and file storage, as determined by the supervising instructor.

e. **Network Etiquette:** Users are expected to abide by the behavior conduct described in the student handbook. Rules that apply "in person" also apply on the network. They should be polite and use appropriate language. Do not use profanity, vulgarities, or any other inappropriate, offensive, harassing, or "stalking" language or behaviors.

f. **Copyrights:** Users may not violate copyright laws or otherwise use the intellectual property of anther individual or organization without the expressed written permission of the owner. The term "owner" includes, but is not limited to authors, publishers, performers, artists, and their agents. Students may employ material under proper use of the "Fair Use" law with permission from the supervising instructor.

g. **On-line activities:** Students may not purchase any goods or services through any CCS provided on-line service. Users may not use the network for commercial gain, product advertisement, or political lobbying.

h. **Personal Privacy:** Students may not reveal their personal name, address, phone number(s), bankcard number(s) , etc. or those of anyone else on line. Users must also be cautious of unsolicited on-line contact and advertising. Report communications that are suspicious or cause discomfort to a CCS Staff member immediately.

i. **Unacceptable Uses:** Users may not access, compose, upload, download, or distribute pornographic, obscene, or sexually explicit material or language. Do not use the network to violate any local, state, federal statute or international law. This includes, but is not limited to, transmission of copyrighted material, threatening or obscene material or material protected by trade secret. Immediately back out of any unacceptable web pages that are accessed and delete any unacceptable files and unacceptable web pages that are accessed and delete any unacceptable files and messages that are received. Students should report this immediately to the supervising instructor so that the site may be blocked and the user will not be held accountable.

j. **Downloads:** Assume that all communications, programs, files, and any other information accessible via the CCS network are private, copyrighted property and respect them as such. Do not upload or download any text or graphic file without doing all the following:

1) Receiving prior authorization by a CCS supervising instructor;

2) Verifying that it is legal to do so under U.S. copyright laws;

3) Making sure each file is not infected with a computer virus.

Other types of files and large graphic files require prior permission of the CCS technology staff.

3. **Piracy --** Most software is licensed and protected by federal copyright law. It is illegal to copy or install protected software without proper license(s). Software may be installed on CCS computers under the following conditions:

a. License requirements regarding the method and number of installations must strictly followed.

b. Software installed on corporation computers is for educational use only and must be approved by the building principal.

c. Software may only be installed by CCS Technology Staff or by staff with the permission of their building principal.

d. A log must be kept of software installed on each machine with the name of the software, date of installation, who installed the software, and the initials of the building principal indicating his/her knowledge that the software was installed and is properly licensed to the corporation.

e. Faculty may install software only on designated faulty and/or student machines.

f. Students are not to install software on corporation computers.

g. No software may be installed on computers in lab setting except by the corporation technicians.

h. Network software must be installed by the corporation technicians.

i. Original program media must be kept in the possession of the corporation.

NO PERSONAL SOFTWARE IS TO BE INSTALLED ON CORPORATION COMPUTERS.

4. **Privileges –** The use of the CCS networks and the Internet is a privilege, not a right and inappropriate use will result in a cancellation of those privileges. The system administrators will judge what is inappropriate use and their decision is final. The system administrators may close an account/password at any time as required.

Administrators, faculty, and other professional staff of CCS may request the system administrator to deny, revoke, or suspend specific user accounts/passwords. Failure to follow the guidelines may also result in disciplinary consequences.

5. **Vandalism –** Vandalism will result in the cancellation of privileges and any additional disciplinary action deemed appropriate. Payment for the repair or replacement of damaged hardware or for services needed to undo software changes may be required of the offender. Vandalism includes but is not limited to defacing, disassembling, or destroying any part of the computer hardware, software, or software settings. Students are not to move any cables, switches, and plugs associated with the computers or network. Vandalism also includes any attempt to harm or destroy data of another user, the CCS network, the Internet, or any other connected agency or network. This includes, but is not limited to, the uploading or creation of computer viruses, programs or files that cause harm.

6. **Security –** Security on any computer system is a high priority, especially when the system involves many users. If a user feels able to identify a security problem on the CCS network, the user must notify a supervising professional or system administrator. Do not demonstrate the problem to other users. Students may not, under any circumstances, use another individual's account. Do not give any passwords to another individual. Attempts to login to the system as any other user may result in suspension or cancellation of user privileges. Attempts to login to

the system as a system administrator will result in 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 CCS network and the Internet.

7. **Privacy –** Users should not expect that files stored on any school-based computer will always be private. Administrators and faculty may review files and messages to maintain system integrity and to ensure that users are acting responsibly. At any point, the network administrator or his/her designee may view an activity log listing web sites visited by each user.

8. **Publishing –** Prior to publication on the Internet, home pages that are intended to represent any school or department of Clay Community Schools must be approved by the Superintendent or his/her designee. All web pages representing Clay Community Schools must follow the Web Page Development Guidelines.

9. **Consequences of Violation(s) –** A violation of the provisions of the AUF or Terms and Conditions may result in revocation of the user's network and/or Internet access privileges regardless of the success or failure of the attempt. In addition, school disciplinary action, including suspension or expulsion, and/or appropriate legal action may be taken.

a. Initial determination: The school administrators with the assistance of the teacher, will make the initial determination.

b. Due process: Violator will be accorded due process rights in the determination of possible violations and consequences.

c. Denial, revocation, or suspension of access: The school administration, in accordance with Clay Community

Schools disciplinary procedures may deny, revoke, restrict or suspend access to CCS networks or Internet.

10. Cyberbullying Education–

a. The Corporation recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about appropriate online behavior, including interaction with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

b. The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

11. **Disclaimer –** Clay Community Schools, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network and Internet access it is providing.

Use of any informationobtained through the Internet is at the users' own risk. Furthermore, CCS is not responsible for:

a. The accuracy, nature, quality, or privacy of information stored on diskettes, hard drives or servers gathered through Internet access;

b. Any damages suffered by a user, including but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries or interruptions in service, computer viruses, or to personal property used to access computers, networks, or the Internet;

c. Unauthorized financial obligations resulting from the Internet access.