Acceptable Use Policy (AUP) ꕥ Employees

We are pleased to offer you, as a staff member of Cincinnatus Central School (CCS), access to the district computer network. To gain access to the district's LAN and wireless network including email, the Internet, telephones, voicemail, messaging including text messages, wireless devices such as iPads, Chromebooks interactive boards, and other devices, all users must sign and return this form to the Personnel Office. The primary purpose of the District's network and Internet connection is educational and professional, and these purposes shall take precedence over all other uses.

- **Privileges:** The use of the district network is a privilege, not a right. Failure to comply with the CCS guidelines of technology use in this document or the district's Board Policy will result in a cancellation of that privilege by the school's Network Administrator, Principals, or Superintendent at any time without warning. This includes (but is not limited to) the following:

- **Netiquette:** All users are expected to abide by the generally accepted rules of network etiquette. The employee is ultimately responsible for his or her own actions accessing technology at CCS.

1. Be polite. Never forget the person on the other end is human.
2. Use appropriate language. Do not swear; use vulgarities, or any other unacceptable language.
3. Be careful with humor and sarcasm.
4. Illegal activities are strictly forbidden.
5. Do not use the network in such a way that you would disrupt its use by other users.
6. Your postings reflect you, be proud of them.
7. Print conservatively to save paper and the environment.
8. Do not stay logged into your computer when unattended. Use CTRL + ALT + Delete to lock the computer.
9. Shut down your computer at the end of the day to reduce carbon emissions and save power.

- **Security Issues:** Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, notify your Network Administrator immediately. Security issues include (but are not limited to) the following:

1. Do not use another's password, this is considered trespassing.
2. Do not leave passwords written down where others may have access to them.
3. Do not leave a computer unattended at anytime that is logged into SchoolTool.
4. Do not give out your password to others. If you are given access to the filter password you are responsible to not give it out to students or others on the network.
5. All communications and information accessible via email or messaging should be considered private property, but is not guaranteed private. CCS does not grant any ownership, privacy, or an expectation of privacy in the contents of any message, including email, messaging or other Internet activities involving CCS resources or equipment when using the CCS network.
6. Data files stored on the school server, USB drives, network drives, or other CCS equipment are not guaranteed private.
7. Do not reveal online the personal address of students or colleagues.
8. Do not conduct online chats with others, only ones for educational purposes.
9. Do not change computer files that belong to another user.
10. Do not falsify your identity.
11. Do not send anonymous messages, forge messages, or use an account owned by another user.
12. The school recognizes that employees may use of Facebook, Twitter, Instagram, Snapchat, TikTok, LinkedIn, and other such social networking applications, blogging and messaging services for educational purposes. Employees must not post material (including text, video, audio or images) which damages the reputation of the school and which could be considered as inappropriate or harmful to others and in some cases is criminal.
13. Do not forward a message that was sent to you privately without permission of the person who sent you the message.
14. Adhere to laws, policies, and rules governing computers including but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

- **Using Resources:** Information networks have set limits for capacity. The more users there are on the network, the more congested the network becomes and access to information will take longer. The following guidelines will help ease the congestion:

1. Do not play online games with others on the network or on the Internet unless for educational purposes like eSports.
2. Do not download huge files unless approved by the Network Administrator. Download only information you need.
3. Do not download music unless approved by the Network Administrator for a school project.
4. If you stumble across unacceptable materials or inappropriate pictures while doing legitimate research, avoid this information by immediately leaving the web site.
5. Check your email frequently, delete unwanted messages promptly.
6. Use your school email account and not email provided by free services such as Yahoo mail for school business.
7. Do not send email or text chain messages or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
8. In creating web pages that are posted on the school server, no profane, abusive, or impolite language should be used to communicate or that would bring harm to others nor should materials be posted which are not in line with the rules stated on this AUP and in accordance with school rules.
9. Do not bring in personal devices such as laptops and connect to the district network without the permission of the Network Administrator.

- **Vandalism/Harassment/Unauthorized Access to Private Information or Files:** will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, or Internet network. This includes, but is not limited to, the uploading or creation of computer viruses. Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes but is not limited to the sending of unwanted email. Unauthorized access to private information means attempting to access the information of another individual of whom you have no legal authorization. Private information includes SSN, Driver's License number, other Identification numbers, account numbers, or security codes and passwords. Private information does not include publicly available information. In addition, you will be in Breach of the Security System if you attempt unauthorized access of another's personal files stored on the school server.

- **Commercial Services:** are available on the Internet. If you choose to access any additional pay per minute services, you are liable for any costs that may be incurred.

■ ■

Acknowledgment of Responsibilities

By signing this document, I understand and will abide by the above terms and conditions for access to the CCS district's LAN and wireless network and any further amendments to the district's AUP or related Board of Education policies. Likewise, I am expected as a teacher or staff member to set a good example for the students by upholding these regulations and helping to enforce these rules with all students UPK-12. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my Internet account may be closed and school disciplinary action may be taken and/or appropriate legal action.

Job Title _____

Department/Office_____

Name (please print) _____ Signature _____ Date _____