

# Acceptable Use Policy (AUP) © Students Grades 5 -12



We are pleased to offer students of Cincinnatus Central School (CCS), access to the district computer LAN network and wireless devices such as iPads. To gain access, including email, the Internet, messaging, phones, and other devices, all students under the age of 18 must obtain parental permission and sign and return this form to the Network Administrator or a computer teacher. Students 18 and over may sign their own forms. The primary purpose of the District's network is educational, and educational purposes shall take precedence over all other uses.

The Internet **Acceptable Use Policy** is one way that we may work together to enforce safe travels on the Internet. The District is also in compliance with the **Children's Internet Protection Act** signed into Federal law by certifying that the district uses a filtering program to protect students against access to visual depictions that are obscene or other content harmful to minors on school computers.

▪ **Privilege:** 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, the Student Handbook, 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 student 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 polite language which also applies when using symbols and text abbreviations. Do not swear; use vulgarities or any other unacceptable language.
3. Be careful with humor and sarcasm.
4. Illegal activities are strictly forbidden and enforced by law.
5. Do not use the network in such a way that you would disrupt its use by other users.
6. Be brief to save cyberspace.
7. Your postings reflect you, be proud of them.
8. Print conservatively to save paper and the environment.
9. Do not type in ALL CAPS it appears that you are shouting.

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

1. Do not use another's password nor give out your password to others, even your best friend.
2. All communications and information accessible via email should be considered private property, but is not guaranteed private.
3. Data files stored on the school server, USB drives, CDROMs, network drives, or other CCS equipment are not guaranteed private.
4. Do not reveal your personal address or phone number, social security number, or those of others.
5. Should you be required to give out your personal contact information such as in an online registration form, you must have parent or guardian written permission first. (A good example may be an online college application. A bad example would be a form to receive free merchandise.)
6. Social networks such as Facebook, Twitter, and Instagram, are not to be accessed on school computers unless given permission by a teacher or network administrator for a school project.
7. The school recognizes that students actively use Facebook, Twitter, Instagram, and other such social networking sites, blogging and messaging services. Students must not post material (including text, video, audio or images) which damages the reputation of the school or post material, which could be considered as inappropriate or harmful to others under any circumstances and in some cases criminal.
8. Do not intentionally access, transmit, copy, or create material that violates the school handbook rules (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
9. Do not conduct online chats with others through live chats or Skype unless given permission by a teacher or the network administrator.
10. Do not change computer files that belong to another user.
11. Do not falsify your identity, be honest.
12. Do not send anonymous email messages, forge email messages, or use an account owned by another user.
13. Do not forward a message that was sent to you privately without permission of the person who sent 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.
15. Users will not attempt to gain unauthorized access to the network or to any other computer system through the school network or go beyond the authorized access. This includes attempting to log in through another person's account or access another person's files even if only for the purposes of "browsing."

16. Cyberbullying is the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, intended to harm others and will be enforced by New York State law.

- **Using Resources:** Information networks have set limits for capacity. The more users there are on the network and wireless devices, the more congested the network becomes and access to information will take longer. The following guidelines will help ease the congestion:
  1. Use your access time efficiently. Remember there are many students, teachers, and staff members who need to use the network.
  2. Do not play online games with others on the network or on the Internet. Networks are not designed for computer games.
  3. Do not download huge files unless approved by your Computer Teacher or Network Administrator. Download only information you need.
  4. Do not download music unless approved by your Computer Teacher or Network Administrator for a school project.
  5. Do not search for, read, email, or print joke lists of any nature unless given permission for a school project.
  6. If you stumble across unacceptable materials while doing legitimate research, avoid this information by immediately leaving the web site.
  7. If you have any question to the appropriateness of data or pictures you find online, ask the Computer Teacher or Network Administrator if it is acceptable for a school setting.
  8. Check your email frequently, delete unwanted messages promptly, and stay within your email quota of 5000K.
  9. Only use your school email account and not email provided by free services such as *gmail*.
  10. Do not join list groups that generate several incoming email messages a day. An example may be Home and Garden Experts for garden enthusiasts. Many discussion groups are of high quality, however require more email space than the school server will allow.
  11. Do not send email chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
  12. Do not use the computer to listen to music or radio stations unless approved by your teacher or Network Administrator for school projects. Headphone use must be approved by your teacher.
  13. 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.

- **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 mail. 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 download applications or access these additional services, you are liable for any costs that may be incurred.



**Student 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, Student Handbook, 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.

Student's Name (please print): \_\_\_\_\_ Student's Signature: \_\_\_\_\_ Date \_\_\_\_\_

Student's Grade \_\_\_\_\_ Student's Year of Graduation \_\_\_\_\_

**Parent or Guardian:**

As a parent or guardian of \_\_\_\_\_, I have read the terms and conditions for Internet access. I understand that this access is designed for educational purposes and the Cincinnatus Central School District has taken available precautions to eliminate controversial materials. However, I also recognize it is impossible for the Cincinnatus Central School District to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Parent or Guardian's Name (please print): \_\_\_\_\_ Parent or Guardian's Signature: \_\_\_\_\_ Date \_\_\_\_\_