

INTERNET USAGE AND EQUIPMENT AGREEMENT

Access to Technology Resources Policy

In order to enhance educational opportunities for its students and for employees to be able to work in a professional and intellectually-stimulating environment, it shall be the policy of the Oneonta City Board of Education to permit access to and use of developing technology equipment and resources, including but not limited to, the Internet. Such access and use shall be restricted to faculty, students, and other persons who are engaged in bona fide educational and administrative activities which serve and are consistent with identified educational objectives and authorized support functions. To those ends, the Oneonta City Board of Education is authorized to establish and impose reasonable rules and regulations regarding access to and use of school-based technology equipment and resources and to require adherence to said rules and regulations through such means as the "Internet Usage and Equipment Agreement" and by the application of appropriate disciplinary policies and procedures.

Statement of Caution and Consequences

Board policy restricts access to and use of technology equipment and resources, including the Internet, to instructional and related purposes with the intent to further educational goals and objectives. However, because of the nature of the technology, it is impossible to ensure that a user's intent upon doing so will not be able to gain access to unsuitable material and data through misuse of computers or the Internet. Oneonta City Schools (OCS) system subscribes to a filtering service to filter or block inappropriate Internet access. Thus, it is the intention of OCS that all technology resources will be used in accordance with any and all school system policies and procedures as well as local, state and federal laws. Internet activity can and will be monitored, along with other aspects of technology usage. Successful or unsuccessful attempts to bypass the Internet filter, misuse of equipment, access to prohibited sites by using proxies or other resources are a violation of this agreement and may result in denial or cancellation of access privileges and are subject to disciplinary action in accordance with the Code of Student Conduct and other applicable policies and regulations. Users are also subject to any civil penalties or criminal sanctions that may arise from unlawful use of the Internet.

Regulations Regarding the Use of Internet Resources

1. Acceptable Use. The use of technology equipment and resources, including the Internet, must be in support of education or research, through the provision of unique resources and opportunities for collaboration among students, teachers and administrators. Use of the Internet must be in support of this and consistent with the educational objectives of the school. Non-educational use may be limited by faculty/staff. Transmission or receipt of any material in violation of any state or federal law is prohibited.

2. Privileges and Expectations of Users. The use of equipment, the OCS network and the Internet is a privilege, not a right, and unauthorized, abusive or inappropriate use may result in restriction or cancellation of those privileges. Users are expected to take proper care of technology equipment and resources. Users of the network will not use their account to obtain, post, view, download or otherwise gain access to potentially objectionable materials such as any defamatory, inaccurate, abusive, violent, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. Such conduct would include, but is not limited to, placing unlawful information on or through the schools' computer network, accessing another person's files or e-mail, and using obscene, abusive, or otherwise objectionable language or images in either public or private files or messages. Users of OCS technology resources must be aware that OCS cannot assume any liability arising out of the illegal or inappropriate use of technology resources.

Students and staff are responsible for appropriate, good behavior on school computer networks and the Internet just as they are in a classroom or on school property. General school rules for behavior and communication apply. It is understood that parents/guardians of minors are responsible for setting and conveying the values that are above the school standards that their children should follow when using media and information sources. Because communications on the network, e-mail, chat rooms and other forms of direct electronic communications are often public in nature, all users should be careful to maintain appropriate and responsible standards. There can be no assurance that e-mail or other forms of direct electronic communication will be confidential and/or private. All users should be aware that information sent via e-mail, in documents, or other means are considered legal documents and can be subpoenaed. All correspondence should be professional in nature. All staff members should follow appropriate behavior standards and maintain the utmost professionalism when posting information on social media sites, web-sites, and during any personal communication relating to school, student, or personal issues whether it is through the OCS network or an outside network.

Safe Internet practices should always be followed. Never disclose personal information and never plan to meet anyone encountered online. Access to network service will be provided only to students and employees who agree to act in a considerate and responsible manner. To that end, OCS supports and respects each family's right to decide whether or not to apply for independent access. To gain access, all students must obtain parental permission and must sign and return the Internet Usage and Equipment Agreement form. All employees must sign the Internet Usage and Equipment Agreement Form.

3. Personal Devices. These Internet usage and equipment policies and procedures pertain to technology equipment personally owned by school employees and students which are brought into school facilities. All personal technologies used on the OCS campus are subject to this agreement and may be used only if such use is in compliance with all school system policies, procedures, and guidelines as well as local, state and federal laws. (This also includes any external storage medium including Dropbox, Google Docs or similar online storage.) Staff and students are required to sign the Internet Usage and Equipment Agreement to gain access to the OCS network, the Internet, and other technology resources. Attempts to circumvent defined procedures to access to the OCS network on personal devices without proper authority may result in disciplinary action for students or staff. OCS is not responsible for any hardware or software damage or repair to personal devices on the OCS network.

4. Network and E-Mail Guidelines. OCS network and Internet users are expected to abide by the generally accepted rules of network etiquette and are expected to act in a considerate and responsible manner. The following infractions are not permitted on any OCS computer, computer network, personal device accessing the OCS network, the Internet or any technology resource. This list is not all-inclusive; discretion should be used at all times.

- a. Sending, displaying, posting or downloading offensive, profane, obscene, pornographic, disrespectful, threatening, or prurient messages or pictures.
- b. Harassing, insulting, embarrassing, threatening, bullying or attacking others or their work.
- c. Using obscene, racist, profane, discriminatory, threatening or inflammatory language in a document, email, web-site, posting, etc.
- d. Using a digital camera, camera phone, or any other device capable of storing a still or video image to take inappropriate and /or embarrassing pictures. Editing or modifying digital photos with the intent to embarrass, harass or bully.
- e. Posting any false or damaging information about other people, the school system, or other organizations.

- f. Damaging computer equipment, any technology resource, computer systems, computer networks, or documents created by other users. This includes changing workstations and printer configurations.
- g. Violating copyright laws. Plagiarizing computer-copyrighted materials constitutes inappropriate behavior.
- h. Use of technology resources to create illegal materials (i.e. counterfeit money, fake identification, etc.) or illegal activities (i.e. threats, instructions of how to perform an illegal act, any form of pornography, drug dealing, purchase of alcohol, gang activities, or any illegal or inappropriate activity).
- i. Using another user's password.
- j. Accessing or trespassing in another user's files, folders, or work or any form of 'hacking.'
- k. Intentionally wasting limited resources.
- l. Disrupting the use of the network by other users.
- m. Uploading or creating computer viruses, malware or spyware.
- n. Re-posting non-academic, personal communications without the original author's prior consent.
- o. Installing software or downloading unauthorized files, music, games, programs or other electronic media onto a workstation, laptop, network drive or any other technology device.
- p. Attempts to circumvent network security or internet access restrictions by any means.
- q. Revealing personal information (i.e. photographs, addresses, or telephone numbers).
- r. E-mailing outside the school system or storing/saving on external storage drives or portable devices that do not remain on campus, electronic copies of student or staff personal information. This information includes, but is not limited to data containing social security number, information protected by FERPA, and any other sensitive and/or protected information.
- s. Using the network for commercial or political purposes.
- t. Ordering anything from the Internet is strictly prohibited by students. Any charges incurred would have to be paid by the user and are not the responsibility of the school.

5. Security

- a. As a registered user of this network, users are responsible for the use of their account and password. Users may only log on to the network with their assigned user name and password. Users should not disclose their password to anyone. If a user feels that their password has been compromised, the user should notify the technology staff immediately. Unauthorized access, including "hacking" is prohibited.
- b. Users who discover or suspect a security problem should notify the teacher, the technology staff, or principal, and should not discuss the problem with or demonstrate it to other users.
- c. Any user who receives threatening or unwelcomed communications or encounter materials that violate the school code of conduct should immediately bring them to the attention of an administrator, teacher, or the technology staff.
- d. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

6. Procedures for Use

- a. In addition to a signed Internet Usage and Equipment Agreement form, student users must have permission from their instructors before using computers, the Internet, or related technology equipment or resources.
- b. Users may not play games or use computer resources for non-academic activities unless given permission to do so by the teacher, superintendent, administrators, or technology staff.
- c. Users may not waste or take without permission supplies (such as paper, printer cartridges, external storage devices, etc.) that are provided by OCS.
- d. No user of electronic media may purchase and/or install technology hardware or software without the written approval of the technology staff.

- e. Damage or vandalism of any technology resource including, but not limited to, equipment, computer networks, or programs will result in punishment as defined in the school conduct policy.
- f. Any use of technology resources that reduces the efficiency of use for others can be considered a violation of this agreement.

7. Oneonta City Schools Domain

- a. Any and all devices connected to the OCS network are considered to be in the private domain of OCS.
- b. Any and all devices connected to the OCS network are subject to inspection, search and monitoring by the superintendent, administrators, or appropriate members of the technology staff, including data stored by individual users on individual school or personal devices. Users should be aware that activities might be monitored at any time, without notice.
- c. All network activity is logged and subject to review by the superintendent, administrators or technology staff members periodically.
- d. No information or resource connected to the OCS network should be considered personal or private from the appropriate members of the technology staff, administrators or superintendent.
- e. Rules and regulations of system usage will be modified, added, and posted from time to time by the administrators of the OCS network. Users of the network are subject to these additional rules and regulations.
- f. All users have a right to privacy. However, if a user is believed to be in violation of the guidelines, the superintendent, administrators or technology staff members may review communications to maintain system and network integrity and to insure that students and staff are using these resources responsibly.