

TECHNOLOGY ACCEPTABLE USE POLICY



The Carroll School Computer Network (the “CarrollNet”) is established for the educational and professional use of Carroll School students, faculty, and staff (“Users”). This Technology and Acceptable Use Policy (the “Policy”) is intended to govern Users with respect to CarrollNet and the Internet. In addition to this Policy, Carroll School regulates access to and use of the CarrollNet by principles consistent with the educational mission of the Carroll School, and the rules and expectations published elsewhere (i.e., Student, Parent, or Faculty Handbook). Users are expected to conduct themselves on the CarrollNet in the same fashion as they do elsewhere in the community. Users who violate this Policy will have their CarrollNet privileges revoked and may be subject to further disciplinary action, including suspension or dismissal. Carroll School may also report offenders to applicable law enforcement agencies.

The CarrollNet provides access to the global Internet. Carroll School has taken available precautions to restrict access to controversial materials on the Internet. However, on a global network, it is impossible to control all materials. Carroll School believes that the valuable information and interaction available on the Internet far outweighs the possibility that Users may find material that is not consistent with our educational goals.

The smooth operation of the CarrollNet relies upon the proper conduct of all Users. The signature on the Handbook Acknowledgement form and Laptop Contracts are legally binding and indicate the



parties who have signed have read the terms and conditions of this Policy carefully and understand their significance.

CarrollNet - Terms and Conditions (Acceptable Use and Illegal Actions)

Scope and Authority – The CarrollNet includes all hardware, software, and network services used by the Carroll community, including third party services that act as extensions of our internal network.

Parents give the school permission to use applications that are educationally beneficial to our students.

Privileges

The use of the CarrollNet is a privilege, not a right. The use of an account must be consistent with the educational objectives of Carroll School. The Technology Office will deem what is inappropriate use and will refer any such conduct to Carroll School Administration. Carroll School, in its sole discretion, reserves the right to determine what conduct constitutes a violation of this Policy, and the discipline for any such violation. In addition, use of any other Internet connected resource must comply with the rules appropriate for that resource. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to, material protected by copyright, threatening or obscene material, or material protected by trade practice. Use of the CarrollNet for commercial activities, product advertisement, or political lobbying is prohibited. Use of the CarrollNet and the Internet must be consistent with this Policy and all policies and practices of Carroll School, and violations of this Policy and such other policies and practices may result in the suspension or loss of an account, loss of Internet access, or in other forms of disciplinary action.

No Expectation of Privacy

Carroll School routinely monitors usage of CarrollNet and may review any communications on its systems. Carroll School is able to override all passwords. **Users do not have a privacy right in the contents of their computer system, including messages sent, received, or stored on the email systems or in their use of the Internet.** Passwords to these systems exist for the benefit of Carroll School. Users should have no expectation that the ability to choose a password for a system in any way limits the ability or right of Carroll School to monitor all activity.

Security

Security on any computer system is a high priority, especially when the system involves many Users. No User may have access to another's files on the CarrollNet. The following guidelines will help maintain CarrollNet security:



- If you feel you have identified a security problem on the Internet, you must notify the Director of Technology.
- Do not allow anyone else to use your account and do not use another individual's account.
- Inappropriate attempts to access a server as an administrator will result in immediate cancellation of User privileges and/ or discipline.
- Any User identified as a security risk or having a history of problems with other computer systems may be denied access to the CarrollNet.

Inappropriate Access

Not all of the information freely available on the Internet is reliable or helpful. Students and employees must evaluate the source of the information, as well as the information itself, to determine its appropriateness and usefulness.

In addition to providing information, the Internet is capable of providing the means to communicate directly with others via “instant or private messaging” programs, video conferencing programs, and other means. Also, there are many places and software technologies that will allow for the free exchange of files between computers over the Internet, such as email. **Not all of these methodologies are appropriate for an educational environment as outlined in this document.**

Downloading or loading of software on Carroll School's computers is prohibited. There is an enormous quantity and variety of free software available on the Internet. However, widespread downloading of such software on the School's computers has a cumulative negative effect, and can result in the substantial degradation of performance, additional maintenance time, and increased threat of virus infestation.

Students may not use school computers to access any Internet site or sites that contain information that is inappropriate for educational purposes or sites that teachers, staff or administration deem inappropriate for the instructional program. Examples of inappropriate information and/or content include, but is not limited to, the following.

Students may not access, upload, download, transmit, display or distribute:

- a.) offensive material – content that is in poor taste or could be considered obscene; abusive or sexually explicit language, racist, illegal, harassing or inflammatory.
- b.) distribute dangerous material – content that provides direction in the construction of explosives or similar devices or instruction or practices that could injure the students themselves or others.
- c.) inappropriate contacts – materials that can lead to contact with strangers who could potentially threaten the student's health or safety.



If a student is uncertain as to whether or not a site's material might be considered inappropriate, the student should consult their teacher or a member of the administrative staff for clarification.

Google Apps for Education Acceptable Use

Google Apps for Education is primarily for educational use. Students may use Google Apps for Education for personal use subject to the restrictions below and additional school rules and policies that may apply. Student accounts are limited to communication inside of the Carroll School (i.e. with Faculty, Administrators, students, etc.).

Privacy

School staff and administrators have access to student email for monitoring purposes. Students should have no expectation of privacy on the Google Apps for Education system.

Limited personal use - Students may use Google Apps for Education tools for personal projects but may not use them for:

- Unlawful activities
- Inappropriate sexual or other offensive content
- Threatening another person
- Misrepresentation of Carroll School, staff or students.

Safety

- Students will tell their teacher or other school employee about any message they receive that is inappropriate or makes them feel uncomfortable.
- Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account.
- Under no conditions should a user provide his or her password to another person.

Access Restriction - Due Process

Access to Google Apps for Education is considered a privilege accorded at the discretion of Carroll School. Carroll School maintains the right to immediately withdraw access and use of Google Apps for Education when there is reason to believe that violations of law or school policies have occurred. In such cases, the alleged violation will be referred to the Head of School for further investigation and account restoration, suspension, or termination. As a party of the Agreement with Google, Carroll School also reserves the right to immediately suspend any user's account suspected of inappropriate use. Pending review, a user account may be terminated as part of such action.



Due to the rapidly changing technology environment, Carroll School reserves the right to determine if an action not listed in this document is inappropriate, and the student may be subject to discipline.

Hardware

Carroll School computers are managed in order to allow for students to use the systems only for educational purposes. Under no circumstances is a student to attempt to modify the existing hardware configuration of the Carroll School computer, either by opening the case or changing hardware settings. Students are responsible for reporting any damage discovered on school computers to their teacher immediately.

*It is specifically set forth in this policy that under NO circumstances are either students, staff or visitors allowed to connect their own personal computers, laptop or notebook computers or any other electronic device to any of Carroll School computers or to the Carroll School internal network, without the expressed knowledge and written consent of the Director of Technology or his/her designee.

Plagiarism

Information obtained from the Internet as part of a research project must be attributed to its source, using a standard bibliography notation. Students and staff may not violate a copyrighted source, or otherwise use another person's intellectual property without his or her prior approval or proper citation.

Contact

Each student and employee is responsible for all activity that occurs under his/her user account. Students and employees may not place information on the Internet that would fall under the category of "unacceptable sites" listed above.

Students may not give out any personal information (e.g., address, phone number, user name, passwords, etc.) about themselves or about other people. Students may not use school computers for commercial purposes or political lobbying.

Summary of Inacceptable Uses

This is a list of the more common things students, faculty and staff are specifically NOT permitted to do.



1. Download any files, especially music and videos, from the Internet, unless the material is free for commercial use and royalty free.
2. Use any form of “instant or private messaging” software.
3. Install any applications or software onto Carroll School computers.
4. Disable or modify any running tasks or services.
5. Transfer and/or store music files from any personal devices to Carroll School systems.
6. Play games, unless directed to by an instructor or supervisor for educational purposes, at any time on Carroll School computers, including Internet-based games.
7. Use proxies or other means to bypass the content filtering systems in place and or defeat any settings that prevent the access of material deemed and flagged as inappropriate by the blocking devices.
8. Use remote accessing software or hardware to take control of any network attached device or workstation.
9. Remove License decals or inventory control tags attached to the systems.
10. Disrupt its use by other individuals by connecting to other Carroll School networks to perform any illegal or inappropriate act, such as an attempt to gain unauthorized access to other systems on the network.
11. Everyone must honor copyrights and licenses, as well as the legal rights of the software producers and network providers.
12. Use of another person’s user account and any access of credentials is prohibited.
13. Anyone who inadvertently accesses an inappropriate site must immediately leave the site and report it to his/her instructor or supervisor.
14. Attempt to log onto the network as a system administrator.
15. Any user identified as a security risk may be denied access to the network.
16. Damage caused by the intentional misuse or vandalism of equipment will be charged to the person who committed the act.

Consequences

Use of school’s internet is a privilege. Failure to abide by the terms of this policy will result in the following disciplinary actions:

Willful damage of computer hardware, computer software (including the deletion of programs and/or files) and computer networks will result in the student being responsible for the current repair and replacement cost of the damaged software and/or equipment. Any student violating the terms of this document will receive appropriate disciplinary action. As defined in the student handbook (under “Violating Computer Use Policy”) students could lose computer/network privileges, and/or receive detention, suspension or expulsion.



The Director of Technology or his/her designee may close an account at any time as required. The administration, faculty and staff of Carroll School may make a request to the Director of Technology or his/her designee to deny, revoke or suspend specific user accounts based upon violations of this policy.

Improper Use and Content

Users may not use the CarrollNet for purposes of harassment, intimidation or bullying of others.

Bullying is the repeated use of a written, verbal or electronic expression, physical act or gesture, or any combination thereof, directed at another student that:

- causes physical or emotional harm to the student or damage to the student's property;
- places the student in reasonable fear of physical injury or of damage to property;
- creates a hostile environment at school for the student;
- infringes on the rights of the student at school; or,
- materially and substantially disrupts the education process or the orderly operation of a school.

A hostile environment is a situation in which bullying causes the school environment to be permeated with intimidation, ridicule or insult that is sufficiently severe or pervasive to alter the conditions of the student's education.

Cyber-bullying involves an act of bullying through the use of technology or any electronic communication, including but not limited to electronic mail, internet communications, or instant messages. Cyberbullying also includes the creation of a web page or blog in which the creator assumes the identity of another person; or, the knowing impersonation of another person as the author of posted content or messages, if the creation or impersonation creates any of the conditions described in the definition of bullying. Cyberbullying also includes the distribution by electronic means of a communication to more than one person or the posting of material on an electronic medium that may be accessed by one or more persons, if the distribution or posting creates any of the conditions described in the definition of bullying.

Carroll School shall, in its sole discretion, determine whether such conduct violates this Policy and any other policies of Carroll School. Users must remember that material distributed through the Internet is public. On the Internet, there is no central authority, so each site is responsible for its own Users. Complaints received from other sites regarding any of our Users will be fully investigated, and disciplinary action may be taken as a result.



Social Networking Sites

While Carroll School respects the proper use of and participation in social media and networking sites, as well as personal websites and blogs, it is important that any such personal use of these sites does not damage Carroll's reputation, and does not directly or indirectly cause harm to the school's employees, students, or families. Student use of non-Carroll social networking sites is prohibited on Carroll distributed laptops. For students, these guidelines apply to personal computer use outside of school. Carroll may monitor use of social media by students and may request access to a student's social media accounts, especially where a problem is brought forward to the attention of the school. Students may be disciplined for social media use or communication occurring during off hours.

All members of the community should understand that Carroll takes seriously, and reserves the right to address, any inappropriate use of social media that may impact the educational environment. All users should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding that what is private in the digital world often has the possibility of becoming public, even without their knowledge or consent.

Carroll School strongly encourages all employees, students and families to carefully review the privacy settings on any social media and networking sites they use (such as Facebook, Instagram, Snapchat, MySpace, Twitter, Flickr, Google+, LinkedIn, etc.), and exercise care and good judgment when posting content and information on such sites. When using a social media site, an employee may not include current students as "friends," "followers" or any other similar terminology used by various sites. If an employee has a community that extends to persons who are parents, alums, or other members of the Carroll School community, s/he must exercise good judgment about any content that is shared on the site.

Additionally, employees, students and families should adhere to the following guidelines, which are consistent with Carroll School's community standards on harassment, student relationships, conduct, professional communication, and confidentiality:

- Users should not make statements that would violate any of Carroll School's policies, including its policies concerning discrimination or harassment;
- Users must uphold Carroll School's value of respect for the individual and avoid making defamatory or disparaging statements about the School, its employees, its students, or their families;
- Users may not disclose any confidential information of Carroll School or confidential information obtained during the course of his/her employment, about any individuals or organizations, including students and/or their families.

Carroll School has a strong interest in promoting a safe and supportive learning environment, as well as maintaining a positive reputation in the community. If the School believes that an employee's activity on a social networking site, blog, or personal website may violate the School's policies or



otherwise may have a detrimental impact on the learning environment, the School may request that the employee or student cease such activity. Depending on the severity of the incident, the employee or student may be subject to disciplinary action. Carroll School reserves the right to impose discipline, up to dismissal or termination, for any behavior on or off campus that Carroll determines may impair or negatively impact the reputation of the School.

Theft and Vandalism

Users must acknowledge the use of the intellectual property of others. Users must treat information found electronically in the same way as information found in printed sources. Rules against plagiarism will be enforced. It is the responsibility of each User to comply with the terms and condition for the acquisition and use of software found on the Internet. Carroll School will not allow the copying or storing of illegally acquired software. In this case, vandalism refers to deliberate attempts to damage the hardware, software, or information residing on CarrollNet or any other computer system attached through the Internet. Attempts to violate the integrity of private accounts, files or programs; the deliberate infecting of a computer with a “virus”, attempts at “hacking” computers using any method, or other such actions shall be a violation of this Policy.

Chain Letters and Other “Spreading” Schemes

Whether in e-mail or in newsgroups, chain letters, pyramid schemes, forwarding or replying to “contests” or “fast cash” schemes, mass cross-postings, and uninvited mass mailings are forbidden on the Internet and on the CarrollNet.

“Netiquette”

Users must abide by accepted rules of network etiquette, including, but not limited to, the following:

- Do not reveal personal information – your address or telephone number, or those of students or colleagues.
- Be polite. Do not be abusive in your messages to others. Use appropriate language and do not use vulgarities, or any other inappropriate language.
- Do not use the CarrollNet in such a way that would disrupt its use by others.

Waiver of Warranties; Limitation of Liability

Carroll School makes no warranties of any kind, whether express or implied, concerning this service. Carroll School shall not be held responsible for any damages suffered, including the loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions, or errors and omissions. Carroll School denies any responsibility for the accuracy or quality of information obtained through



this service. All terms and conditions as stated in this Policy are applicable to the use of computer resources at Carroll School, in addition to internet use.

Entirety of Agreement

The terms and conditions stated in this Policy, and all other policies of Carroll School incorporated herein, reflect the entire agreement of the parties with respect to the subject matter stated herein. This Policy supersedes all prior oral or written agreements and understandings of the parties. This Policy shall be governed by and interpreted in accordance with the laws of the Commonwealth of Massachusetts and the United States of America.

Preservation of Resources

All resources are limited; computer resources are not an exception. Because space on disk drives and bandwidth across the lines, which connect CarrollNet both internally and externally, are limited, neither programs nor information may be stored on the system without the permission of the system administrator. Users are not to load software on any school computer. Each User is permitted reasonable space to store e-mail, Web, and personal files, as mandated by system file quotas. Carroll School reserves the right to require the purging of files in order to regain disk space without warning. Users whose need for the resource is more pressing will have priority of space.

Special Note Regarding Borrowed Equipment

Because Carroll is a day school, and for the convenience of the user community as a whole, Carroll School provides computers, digital still cameras, digital video cameras, and other equipment for student use. Users are responsible for any equipment they may borrow, including accessories, and are expected to employ the equipment in accordance with this Policy. If the equipment should be damaged, or lost while the User has assumed responsibility for it, the User will be accountable for the fair replacement value of the equipment.

