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") outlines the expectations for all Users when interacting with Carroll School's technology resources, including the school network, devices, applications, and internet access. All use must be consistent with the educational mission and values of Carroll School. Users are expected to demonstrate responsible digital citizenship and conduct themselves with the same high standards of behavior and respect online as they do in all other areas of the Carroll School community. Violations of this Policy will result in the immediate revocation of technology privileges and may lead to further disciplinary action, including but not limited to, suspension or dismissal from the school. The Carroll School reserves the right to report serious offenses to applicable law enforcement agencies.

Carroll School provides access to the global Internet to support learning and professional development. While we utilize filtering and security measures to minimize exposure to inappropriate or harmful content, it is impossible to control all materials on the internet. We believe the vast educational benefits and opportunities for positive interaction on the internet outweigh the inherent risk that Users may encounter content inconsistent with our educational goals. Users share the responsibility for navigating online content safely and ethically.

The successful and secure operation of the CarrollNet depends on the proper conduct of all Users. By signing the Handbook Acknowledgment form (and/or any specific technology agreements), Users and their parents/guardians confirm they have read, understand, and agree to abide by the terms and conditions of this Policy.

Scope and Authority of CarrollNet
This Policy governs the use of all technology resources provided by or accessible through Carroll School, including:

- All school-owned hardware (e.g., Chromebooks, computers, peripherals) and software.
- The Carroll School network, including wired and wireless connections.
- All online services, applications, and platforms utilized for educational or professional purposes, including third-party services that integrate with or extend the school's learning environment (e.g., Google Workspace for Education, specific educational apps).
- Any personal devices (BYOD) when connected to the Carroll School network or used for school-related activities on school property.

The school reserves the authority to manage, monitor, and enforce this Policy across all these technology resources. Parental/caregiver permission, as detailed in the "Parental Consent and

COPPA Compliance" section, is integral to the school's ability to provide and utilize various educationally beneficial applications and services for students.

Privileges
Use of the CarrollNet is a privilege, not a right, and must align with the educational mission and values of Carroll School. The school, through its designated administrators, reserves the sole right to determine what constitutes inappropriate use or a violation of this Policy, and to apply appropriate disciplinary action.

All use of school technology and connected Internet resources must comply with this Policy, all other Carroll School policies and practices, and applicable U.S. and state regulations. Prohibited activities include, but are not limited to:

- Transmission, access, or distribution of material protected by copyright, trade secret, or other intellectual property laws without authorization.
- Display, transmission, or distribution of threatening, harassing, obscene, sexually explicit, or otherwise inappropriate content.
- Use for commercial activities, product advertisement, political lobbying, or personal financial gain.
- Any activities intended to disrupt the network, damage equipment, or gain unauthorized access to systems or data.

Violations of this Policy may result in the immediate revocation of technology privileges, suspension or loss of account, loss of Internet access, and/or other disciplinary action as outlined in the student or employee handbook. Serious offenses may also be reported to law enforcement agencies.

No Expectation of Privacy
Due to the nature of providing technology resources for educational purposes, users should understand that there is no absolute expectation of privacy when using the CarrollNet.

The school monitors the use of its technology resources, including network traffic, stored files, and communications on school-provided accounts and devices. This monitoring is conducted to ensure the security and integrity of the school's systems, to enforce this Policy, to comply with legal requirements, and to promote a safe and appropriate online environment for all users.

Carroll School retains the ability to access and review all data and communications on its systems, including the ability to override user-created passwords. This capability is necessary for technical support, system administration, investigations of policy violations, and compliance with legal requests.

To ensure student safety and well-being, Carroll School routinely monitors student online activity, including internet searches and communications using school-provided accounts and devices. This includes activity within Google Workspace for Education and other educational applications. While the school utilizes various monitoring tools, we acknowledge that no system is completely comprehensive. We make reasonable efforts to monitor student online activities

and will contact parents/caregivers if we become aware of potentially harmful or inappropriate online behavior.

Parents/caregivers are strongly encouraged to actively monitor their children's use of electronic devices, particularly their internet and social media activities, and to establish appropriate restrictions.

Carroll School is committed to protecting student data and complies with all applicable privacy laws, including the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA).

Security
Maintaining the security and integrity of the CarrollNet is a top priority, especially given the number of users and the sensitive nature of school data. All users play a vital role in ensuring a secure and reliable technology environment.

Users must not engage in any unauthorized access to another user's accounts, files, data, or any CarrollNet system. This includes attempts to bypass security measures or gain unauthorized administrative access.

To uphold the security of CarrollNet, all users must adhere to the following guidelines:

- Report Security Concerns: If you identify or suspect any security vulnerability, unauthorized access, or potential threat to CarrollNet (including its systems, data, or user accounts), you must immediately notify the Director of IT or other designated IT staff. Do not attempt to investigate or resolve the issue yourself.
- Prohibited Access Attempts: Any unauthorized attempts to access CarrollNet systems, accounts, or data, or to circumvent security controls, will result in the immediate cancellation of user privileges and significant disciplinary action.
- Access Denial: Any user identified as a security risk, or who has a history of problems with other computer systems or networks, may be denied access to CarrollNet.

Do not allow anyone else to use your account and do not use another individual's account.

Content and Communication Guidelines
CarrollNet provides access to a vast amount of information. Not all information freely available on the Internet is reliable, accurate, or appropriate for an educational environment. Students and employees are expected to critically evaluate the source and content of information to determine its appropriateness, usefulness, and validity.

Users may not use CarrollNet to access, upload, download, transmit, display, or distribute any material that is:

- Offensive or Harmful: Content that is obscene, sexually explicit, abusive, discriminatory (including racist or hateful), harassing, inflammatory, or otherwise inconsistent with the school's values and educational mission. This includes content promoting illegal activities

or extreme ideologies.
- Dangerous or Illegal: Content that provides instruction for constructing weapons, explosives, or other dangerous devices; promotes self-harm; or depicts or encourages illegal acts.
- Threatening or Exploitative: Materials or communications that could lead to contact with unknown individuals who may pose a threat to one's safety or privacy, or that are used to exploit, harass, intimidate, or bully others.
- Violative of Rights: Content that infringes upon copyright, trademark, or other intellectual property rights.

Downloading, loading, or installing any unauthorized software or applications onto Carroll School computers or systems is strictly prohibited. Unauthorized software can degrade system performance, increase maintenance demands, and introduce security risks like viruses or malware.

Users are prohibited from using unauthorized "instant or private messaging" programs, video conferencing applications, or other direct communication tools for personal or non-educational purposes on CarrollNet. The school provides approved communication platforms for educational use, and all activity on these platforms is subject to this Policy.

If you are ever uncertain whether a site's material or a communication method is appropriate, you must consult your teacher or a member of the administrative staff for clarification before proceeding.

Beyond the prohibitions outlined, all users hold key responsibilities for maintaining a safe and appropriate online environment. Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from accessing their account. Under no conditions should a user provide their password to another person. Furthermore, if a student receives any message or encounters any content that is inappropriate or makes them feel uncomfortable, they are required to immediately inform their teacher or another school employee.

Parental Consent and COPPA Compliance
Carroll School is committed to providing students with the most effective and secure web-based tools and applications for learning. To facilitate this while protecting student privacy, the school must comply with federal regulations, including the Children’s Online Privacy Protection Act (COPPA).

Carroll School utilizes various computer software applications and web-based services, many of which are operated by third-party vendors, to support our educational programs. An up-to-date list of these approved software applications and services, along with links to their privacy policies where available, can be found on the Aspen Class Pages and is subject to change throughout the academic year.

In order for students to use these programs and services, certain personal identifying information, typically the student’s first name, last name, their Carroll email address, and username, must be

provided to the web service operator. It is important to note that a student's Carroll email address is restricted and cannot be contacted by individuals or parties outside of the Carroll domain, nor are students permitted to email addresses outside the Carroll domain.

Under federal law (COPPA), websites generally require parental notification and direct parental consent before collecting personal information from children under the age of 13. For more detailed information on COPPA, please visit http://www.ftc.gov/privacy/coppafaqs.shtm.

By providing consent through the submission of the signed parent and student handbook, Carroll School is legally permitted to act as the parental agent, thereby providing consent to these third-party operators for the collection of the aforementioned limited personal identifying information on behalf of all enrolled students. This streamlined process eliminates the need for individual parental consent directly to each web service operator.

Your signed parent and student handbook will explicitly constitute consent for Carroll School to provide this necessary personal identifying information for your child to the operators of approved web-based educational programs and services.

Google Workspace for Education Accounts
Carroll School provides students with Google Workspace for Education accounts to enhance learning and facilitate communication. These accounts are integral to our educational program, used for:

- Classroom assignment distribution and submission.
- Teacher-student communication.
- Access to various educational software and online learning tools.

Carroll Google Workspace for Education accounts are primarily for educational use and are limited for use within the Carroll domain. They cannot be accessed or contacted by individuals or parties outside of the Carroll domain, ensuring a secure and contained learning environment. All CarrollNet policies, including this Acceptable Use Policy, apply to the use of these accounts. Student accounts are deleted 30 days after students leave Carroll School.

While primarily for educational purposes, students may use Google Workspace for Education tools for limited personal projects outside of school hours, subject to the following restrictions and all other applicable school rules and policies. Accounts may not be used for:

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

Access to Google Workspace for Education is a privilege granted at the discretion of Carroll School. The school maintains the right to immediately withdraw or suspend access and use of Google Workspace for Education accounts when there is reason to believe that violations of law, this Policy, or other school policies have occurred. In such cases, the alleged violation will be

referred to the Head of School or other designated administrators for further investigation, which may lead to account restoration, suspension, or termination. As per the school's agreement with Google, Carroll School also reserves the right to immediately suspend any user's account suspected of inappropriate use, pending review.

Use of School-Owned Hardware
Carroll School provides and manages technology resources to support educational and professional purposes. To maintain the integrity and functionality of these systems, users must adhere to the following:

- No Unauthorized Modification: Under no circumstances should a student attempt to modify the existing hardware configuration of any Carroll School computer or device, including opening the case, or changing BIOS or other hardware settings.
- Report Damage: Students are responsible for reporting any damage discovered on school-owned computers or devices to their teacher immediately.
- No Unauthorized Connections: Students, staff, and visitors are not allowed to connect personal computers, laptops, notebooks, personal digital assistants, or any other electronic device to any Carroll School computer or to the CarrollNet without the expressed knowledge and written consent of the Director of IT or their designee.

Student Chromebooks (Lower, Middle, and Upper School)
Carroll School provides Chromebooks to support student learning across all divisions. Specific policies regarding ownership and responsibility apply:

- Lower School Chromebooks: All students in the Lower School program receive a Chromebook for use during the academic year. These Chromebooks remain the property of Carroll School and must be returned annually.
- Middle and Upper School Chromebooks: All students entering the Middle or Upper School program receive a Chromebook for their exclusive use throughout their time at Carroll. These Chromebooks are purchased by the student's family and are not returned yearly. Students are responsible for the safekeeping, appropriate use, and any damage to their Chromebook.

The student and their family are solely responsible for any repair or replacement costs incurred due to damage, loss, or theft of the device. This responsibility extends to all components and accessories.

Middle and Upper School students are responsible for the appropriate use and storage of their family-purchased Chromebooks over the summer. While students are enrolled at Carroll, their Chromebooks remain subject to all existing school policies, including this Technology Acceptable Use Policy.

Preservation of Resources
CarrollNet resources, including disk drive space and network bandwidth, are finite. To ensure equitable access and optimal performance for all users, the following guidelines apply:

- No Unauthorized Software/Information Storage: Neither programs nor information may be stored on CarrollNet systems without the explicit permission of the Director of IT or designee.
- No Software Loading: Users are not permitted to load any software onto school computers or devices.
- File Quotas and Purging: Each user is allocated reasonable space for email, web, and personal files, as determined by system file quotas. Carroll School reserves the right to require the purging of files to regain disk space without prior warning. Priority of resource space will be given to users with the most pressing educational or professional needs.

Borrowed Equipment
For the convenience of the Carroll School community, loaner equipment (such as computers, digital still cameras, digital video cameras, and other devices) may be available for student use.

- User Responsibility: Users are fully responsible for any equipment they borrow, including all accessories, and must use it in accordance with this Policy.
- Accountability for Damage or Loss: If borrowed equipment is damaged or lost while under the user's responsibility, the user will be accountable for the fair replacement value of the equipment.

Responsible Online Conduct & Digital Citizenship
Users are expected to conduct themselves with the highest standards of respect, integrity, and ethical behavior when using CarrollNet, reflecting the values of the Carroll School community. This applies to all online interactions, whether within the school domain or on broader internet platforms, including social media and personal websites and blogs.

Users may not use CarrollNet for purposes of harassment, intimidation, bullying, or any form of abuse towards others, whether within the Carroll School community or the broader Internet. This includes, but is not limited to, using foul, abusive, discriminatory, demeaning, or sexually explicit language; attempts to "fill" electronic mailboxes; posting obscene images or texts; or engaging in "flames" or other disruptive acts. Users must also never give out personal identifying information (e.g., address, phone number, personal email, passwords, etc.) about themselves or others, including any information that could lead to inappropriate contact with strangers or compromise safety. If a student receives any message or encounters any content that is inappropriate or makes them feel uncomfortable, they must immediately report it to their teacher or another school employee.

Finally, users must abide by accepted rules of network etiquette. This includes being polite, using appropriate language (avoiding vulgarities or inappropriate language), and not using CarrollNet in a way that disrupts its use by others.

Social Networking Sites
While Carroll School respects the right of employees, students and families to use 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 School's reputation, its employees, or its

students or their families. Student use of social networking sites is prohibited on Carroll distributed laptops; for students, these guidelines are intended to be applied for personal computer use outside of school. 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, Twitter, LinkedIn, Instagram, Snapchat, TikTok, or any other social media platform), 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/caregivers, alums, or other members of the Carroll School community, they 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 their 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 a student'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 student cease such activity. Depending on the severity of the incident, the student may be subject to disciplinary action. Carroll School reserves the right to impose discipline, up to dismissal, for any behavior on or off campus that Carroll determines may impair or negatively impact the reputation of the School.

Intellectual Property, Plagiarism & Copyright

Users must always acknowledge and respect the intellectual property rights of others. Information obtained through CarrollNet, including from the Internet, that is part of a research project or used in any context, must be properly attributed to its source using standard citation methods. Students may not violate copyrighted material or otherwise use another person's intellectual property without their prior approval or proper citation.

Specific Prohibitions
To maintain a secure, functional, and productive learning environment, users are specifically prohibited from engaging in the following activities on CarrollNet:

- Unauthorized Downloads & Software: This includes downloading any unauthorized files, especially music and videos, from the Internet, unless the material is explicitly free for commercial use and royalty-free. Users are also prohibited from installing any applications or software onto Carroll School computers or devices, or transferring and/or storing music files or other unauthorized media from personal devices to CarrollNet systems.
- Unauthorized Access & System Interference: Users may not attempt to disable or modify any running tasks or services on CarrollNet systems, use proxies, VPNs, or other means to bypass content filtering systems or defeat any settings that prevent access to material flagged as inappropriate by blocking devices. Remote access software or hardware to take control of any network-attached device or workstation is also forbidden. This also includes attempting to log onto the network as a system administrator, disrupting CarrollNet's 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. Users are prohibited from violating the integrity of private accounts, files, or programs, deliberately infecting a computer with a "virus" or other malware, or attempting "hacking" using any method.
- Prohibited Communication Schemes: Engaging in phishing emails, pyramid schemes, forwarding or replying to "contests" or "fast cash" schemes, mass cross-postings, and uninvited mass mailings is forbidden.
- Gaming & Non-Educational Use: Playing games, including Internet-based games, at any time on Carroll School computers is prohibited, unless specifically directed by a faculty or staff member for educational purposes.
- Physical Tampering & Vandalism: Removing license decals or inventory control tags attached to CarrollNet systems is forbidden. Vandalism, defined as deliberate attempts to damage the hardware, software, or information residing on CarrollNet or any other computer system, will result in the person who committed the act being charged for the damage.
- It is the responsibility of each user to comply with the terms and conditions for the acquisition and use of software found on the Internet. Carroll School will not allow the copying or storing of illegally acquired software on CarrollNet.

Policy Enforcement & Consequences
Use of CarrollNet is a privilege, and failure to abide by the terms of this Policy will result in serious disciplinary action. Carroll School reserves the right to impose discipline, up to and including dismissal, for any behavior on or off campus that Carroll determines may impair or negatively impact the reputation of the School or the learning environment.

Willful damage to Carroll School computer hardware, 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. As outlined in the Hardware and Devices section, any damage to family-purchased student Chromebooks is the

sole responsibility of the user and their family. Complaints received from other sites or parties regarding any of our users' online conduct will be fully investigated by Carroll School.

Any student violating the terms of this document will receive appropriate disciplinary action, as defined by the terms of the student handbook and/or the Consequences for Misuses document shared with students. This may include, but is not limited to, loss of CarrollNet privileges, detention, suspension, or expulsion. Finally, any user identified as a security risk or having a history of problems with other computer systems may be denied access to CarrollNet.

Use of Artificial Intelligence (AI)
As AI technologies become increasingly integrated into education and daily life, Carroll School is committed to guiding their safe, effective, and responsible use for student learning. We have established the following core principles:

- Academic Integrity: Students must use AI tools ethically as aids to learning and research, not as substitutes for original thought and effort. All work submitted must remain the student's own, and any use of AI tools must be properly cited and acknowledged according to teacher guidelines.
- Privacy & Security: Any AI use approved by Carroll School will adhere strictly to regulations and best practices protecting student data privacy, safety, and accessibility. Students should only use AI tools explicitly approved by the school, as unapproved tools may not meet our privacy standards.
- Critical Evaluation: Users are responsible for evaluating the accuracy, potential biases, and appropriateness of any content generated by AI. AI outputs should always be viewed critically and verified.
- Continuous Evaluation: We will routinely audit AI use, updating policies, training, and approved tools as needed to adapt to emerging technologies.

Waiver of Warranties; Limitation of Liability
Carroll School provides CarrollNet and its associated technology resources on an "as-is" basis and makes no warranties of any kind, whether express or implied, concerning these services.

Carroll School shall not be held responsible for any damages suffered, including but not limited to the loss of data, resulting from delays, non-deliveries, missed deliveries, service interruptions, or errors and omissions. Furthermore, Carroll School denies any responsibility for the accuracy, quality, or legality of information obtained through CarrollNet or its connected services.