



TECHNOLOGY AND INTERNET USAGE AGREEMENT

ARCHDIOCESE OF WASHINGTON – Catholic Schools

Purpose

Archdiocesan parents, educators, and administrators work together every day to ensure the safety and security of all God's children. With our schools' ever-growing and abundant technology resources, it is more important than ever that we communicate clear expectations of our students. The following guidelines were developed from Archdiocesan curriculum and have been adapted, with permission, from the [International Society for Technology in Education](#). For more information regarding each school's individual rules, please refer to your school policy. Thank you for your consideration and cooperation.

Our schools provide students with an opportunity to access computers and computer networks, including the Internet. Our goal in providing this service is to promote educational excellence in our schools. Access to this technology is a privilege, not a right. All students are expected to abide by the following technology rules and to sign the user agreement.

Students

1. **Students will cultivate and manage their digital identity and reputation and demonstrate awareness of the permanence of their actions in the digital world. T.PK8.DC.1. All Students:**
 - a. Shall always represent themselves in a manner that respects the values of the Catholic Church when using **electronic devices, network** and the **Internet** and demonstrate an understanding that digital content is everlasting, even when deleted or within privacy settings;
 - b. Shall only use accounts assigned to them or authorized by the school, supporting others' positive digital identity by not accessing the accounts of others or falsely representing themselves as others;
 - c. Shall keep all accounts and password information private and secure.

2. **Students will engage in positive, safe, legal and ethical behavior when using technology equipment, including social interactions online or when using networked devices. Students will demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property. T.PK8.DC.2, T.PK8.DC.3. All Students:**
 - a. Shall always demonstrate kind and respectful behavior towards others when using electronic devices, network and Internet; following school policy agreements and [anti-cyberbullying laws](#) at the local, state and federal levels;
 - b. Shall immediately report any known **cyberbullying** behavior to a teacher or supervising staff member;
 - c. Shall protect the rights and privacy of others, by never photographing or filming an individual without consent, and never posting and/or distributing videos or photographs without consent of the school and the persons depicted;
 - d. Shall behave in a safe manner when using **technology** by protecting and not sharing personal information and personal images in the public domain. While on school property, students will only use technology to communicate with individuals within the school community or organizations/experts approved by teachers. While on school grounds students shall only use communication platforms approved by the school and all communication shall be only for educational purposes;
 - e. Shall abide by all copyright and intellectual property laws, avoiding plagiarism by using proper citations or permissions. Students shall only use work product that is their own, not taking credit of the work of others;
 - f. Shall immediately report to a teacher or supervising staff member any inappropriate material or misuse of technology equipment of which the student becomes aware.

3. **Students will manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online. T.PK8.DC.4. All Students:**

- a. Shall protect and **manage personal data** in a safe manner by never posting, or otherwise distributing personal information such as photographs, home addresses, telephone numbers, parents' work addresses or telephone numbers or the name and location of the school;
- b. Shall respect networking protections and security within the school infrastructures by working within the designated login and security parameters and never reconfiguring or hacking any school hardware, software, or network settings;
- c. Shall use school issued email accounts for authorized educational purposes only;
- d. Shall respect the right of the school to monitor student use of technology.

4. Students will treat all technology equipment including **issued devices, software and networking systems with care and respect, whether at school, at home, or elsewhere. All Students:**

- a. Shall demonstrate proper physical care for **technology equipment**;
- b. Shall protect the proper functioning of technology equipment by downloading only teacher approved files and not intentionally writing, producing, generating, copying or introducing dangerous codes or programs designed to cause harm, including, but not limited to viruses, bugs, 'worms', etc.;
- c. Shall respect the digital property of others by not accessing or searching files, directories, or folders for which the student does not have authorization, and by not intentionally erasing, renaming, moving, or disabling anyone else's files or programs;
- d. Shall maintain the settings of any issued device by not manipulating any device settings or functionality.

5. Students understand and acknowledge that:

- a. Any violation of this policy may result in permanent revocation of their technology privileges and other disciplinary action may be taken in the sole discretion of the principal.
- b. Schools may require that technology used in a bring your own device program must meet certain compatibility requirements, use certain security measures, and include certain hardware, software, or applications, which may include applications that grant the school control over the content on the technology.
- c. Use of all technology may be monitored, and there is no expectation of privacy for issued devices, or for any information stored on any technology used on school grounds, including any information or files stored in students' personal accounts (such as social media or file sharing accounts) that are accessible via such technology.
- d. The school reserves the right to maintain, access, or retrieve an issued device at any time, at its sole discretion; the school reserves the right to access a student's computer files or any other technology equipment when required for the maintenance of the school's technology equipment, in emergencies, in the course of investigation of possible wrongdoing, or at the discretion of the principal.

Parent/Guardian

Parent(s)/Guardian(s) shall support both school and ADW-wide policies and procedures as they relate to the use of technology and our Catholic Identity

1. Parent(s)/Guardian(s) will monitor online behavior and social media within the home and notify the school in the event of any incident contrary to the school policy, providing evidence when applicable.
2. Parent(s)/Guardian(s) will monitor their child's use of the Internet when the school networks and accounts are accessed from home or a non-school location
3. Parent(s)/Guardian(s) agree that students' schoolwork should be limited to school authorized accounts only (if provided by the school)
4. Parent(s)/Guardian(s) shall respect the right of the school to monitor student use of technology
5. Parent(s)/Guardian(s) are responsible for all fees as determined by school policy related to loss, damage, or misuse of school technology.

Additional resources related to digital safety and digital citizenship; <https://adwcollaborators.weebly.com/parent-resources.html>

Student & Parent/Guardian Acknowledgement

By signing this agreement, the guardian(s) acknowledge(s) that he or she has read the above expectations and reviewed with the student below. Both parent and student understand and agree to abide by those terms. Violations of this agreement are subject to disciplinary action by the appropriate administrators.

Student's Name

Parent/Guardian Name

Student's Signature

Date

Parent/Guardian Signature

Date

Definitions

Cyber-bullying/Harassment: of others online, whether against a student, non-student, or employee, is serious, is prohibited, and is contrary to the School's policy and values. Harassment/cyber-bullying whether it is initiated on or off campus, online or in person, should be reported immediately to a faculty member, and may lead to disciplinary action and possible criminal prosecution. <https://cyberbullying.org/>

Data-Collection Technology for Tracking Navigation: Entities that track an individual's personal data when using networked devices, for example, website cookies, search algorithms return results based on past searches, website analytics, GPS on cell phones, the "Internet of Things" where data is exchanged between networked devices and objects

Digital Identity and Reputation: How an individual is represented online in the public domain, based on activities, connections or tagging. For example; social media posts, photos, public online comments/reviews, awareness and monitoring of how others are depicting you online

Digital Privacy and Security: For example; activate privacy settings on social media accounts and each engines, recognize sites that use encryption, secure login and password information on shared devices, read and be conscientious about accepting privacy policies and access requests from apps and websites

Educational/Academic Purposes: Those tasks performed by students, which are directly related to the schools curricular assignments, projects or research.

Electronic Device: Any device (personal or school-issued), including, but not limited to desktop computers, laptops, Chromebooks, Smartphones, iPads, tablets and e-Readers.

Ethical Behaviors: Interactions that align with one's moral code, for example, preventing or not engaging in cyberbullying, trolling or scamming; avoiding plagiarism; supporting others' positive digital identity

Legal Behaviors: Interactions that are mindful of the law. For example, abiding by copyright and fair use, respecting networking protections by not hacking them and not using another's identity.

Intellectual Property: Content or ideas created by an individual or entity, for example, music, photos, narration, text and design

Internet: A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Issued Device: Device that is the property of the school and is provided to a student as part of the student's educational program.

Managing Personal Data: For example, creating effective passwords, authenticating sources before providing personal information, sharing personal data conscientiously, not posting address and phone numbers visibly

Network: The system of devices, kiosks, servers, databases, routers, hubs, switches and distance learning equipment.

Online or Networked Devices: For example, internet-connected computers or tablets, multiplayer gaming systems and cell phones

Parent: The biological or adoptive parent, legal guardian or person acting in the absence of the parent or guardian.

Permanence of their actions: Digital content is everlasting; even when individuals delete it or believe privacy settings fully protect them from scrutiny.

Positive Behaviors: Interactions that convey a portrait of the way you want to be perceived and healthy interactions with technology itself, for example, moderating the time online or gaming, ergonomic issues and balancing use of media with daily physical activity.

Rights and Obligations of Using and Sharing: Abiding by copyright and fair use, citing resources, gaining or giving permission to use (content), avoiding plagiarism, understanding and using creative commons.

Safe Behaviors: Interactions that keep you out of harm's way, for example, knowing the identity of who you are interacting with; how much and what kind of information you release online; protecting oneself from scams, phishing schemes and poor purchasing practices (e-commerce theft)

Student Authorized Users: Any student enrolled in this school who is assigned a username and password.

Technology (equipment): Any electronic device or system that uses, stores, manages, carries, or supports audio, video, text or data and includes, but is not limited to, information transmitted or received via radio, television, cable, microwave, telephone, computer systems, networks, copiers, scanners, cell phones/smart devices and fax machines.