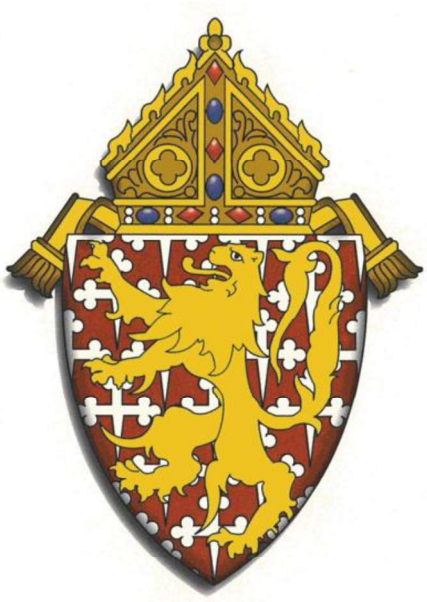
Acceptable Use of Technology in Education

Catholic Diocese of Wilmington

Student Edition

August, 2016



Diocese of Wilmington
Catholic Schools
Acceptable Use of Technology
Student Edition

Table of Contents

Introduction

This Policy applies to students, including students enrolled in aftercare programs and exchange students. All children visiting our campus are also subject to the terms and conditions of this Acceptable Use of Technology Policy.

This policy provides expectations for the use of technology as it affects our school and educational community. The school's computer network is provided for educational purposes, not as a public access service.

The use of all school owned technology is a privilege not a right. This privilege comes with personal responsibilities and if you violate the responsible use of any school technologies, your privilege may be suspended and/or revoked. Our policies address the appropriate use of school-provided technologies and personal technology devices (PTD). Please read the policies below before using our network and computers, because by using our technology you agree to be bound by the terms, conditions and regulations below.

Our school technology users are expected to adhere to the same rules, guidelines, and policies that apply to non-technology related student behavior. If there is an issue about which you are unsure, seek the advice of legitimate authority.

All students and their parent or guardian must sign a parental authorization form before they can utilize any school technologies. This authorization must be signed on an annual basis at the beginning of every school year.

In accord with the Children' Internet Protection Act (CIPA) requirements for schools filing for ERate funding, all schools governed by these policies provide for the education of students regarding these Acceptable Use Policies and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and regarding cyberbullying awareness and response.

Personal Responsibility

Technology is a finite, shared resource offered by the school to its students. Students bear the burden of responsibility to inquire with the IT Department or legitimate authority when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

Purposes and Use Expectations for Technology

- The use of all school-owned technologies including the school network and its Internet connection is limited to educational purposes.
- Commercial, political and recreational use of school technology resources for personal gain is prohibited.
- Students may not resell their network resources to others, including, but not limited to, disk storage space.
- Students may not utilize school technology to play games, visit social networking websites, or send instant messages or emails unrelated to educational purposes. The school is not responsible for any damages, injuries, or claims resulting from violations of responsible use of technology.

Privacy

All communication that takes place using personal technology devices or school owned technology must reflect the mission and values of the school and the Catholic Diocese of Wilmington. This includes, but is not limited to, emails, texts, instant messages, and posts online.

Students should not expect that what they write or publish online is private. The school reserves the right to monitor and track all behaviors and interactions that take place online or through the use of technology on our property or at our events. We also reserve the right to investigate any reports of inappropriate actions related to any technology used at school. All emails and messages sent through the school's network or accessed on a school computer can be inspected. Any files saved can also be inspected. Students have a limited expectation of privacy when using their own technology on school property or at school events as long as no activity violates policy, law and/or compromises the safety and well being of the school community.

Parents or guardians can request permission to see the emails and other data for their child's computer account at school.

School Provided Technology Resources

School provided technology resources can include, but are not limited to, devices owned and/or managed by the school and the school network and internet access.

- Students should be aware that they are sharing resources such as bandwidth and server space.
- Downloading or streaming large files may interfere with Internet speed. Abusing these resources can result in the loss of this privilege.
- Connection to wireless Internet by students is prohibited unless otherwise directed/instructed by legitimate authority.
- Students may not connect or disconnect computers and devices to the school's network.
- Users must log off when finished using a school computer.
- Students are responsible for any activity that occurs through their personal account.
- Students may not use the school's technology to play computer games, unless permission is granted by legitimate authority.
- Students may not download, add, or install new programs, software, or hardware onto school-owned computers without permission from legitimate authority.
- Students are not allowed to alter, change, modify, repair, or reconfigure settings on school-owned computers without permission from legitimate authority. This includes deleting cookies and history and re-setting the time and/or date on the computer.
- Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited.
- Students may not circumvent any system security measures.
- Students are not to share, or try to guess passwords.
- Students are not to access any secured files, resources, or administrative areas of the school network without express permission or the proper authority.
- International websites may only be accessed from school owned technology under the direction of legitimate authority

Accounts and Access Deletion

Upon graduation or other termination of your official status as a student at our institution, you will no longer have access to the school network, files stored on the school network, or your school-provided email account. Prior to graduation, we recommend saving all personal data stored on school technology to a removable hard drive and set up an alternative email account.

Respect for the Privacy of Others and Personal Safety

Students should not:

- modify files, other data, or passwords belonging to others
- misrepresent or assume the identity of others
- re-post information that was sent to you privately without the permission of the person who sent you the information
- post private information about another person
- post photos or videos of others without prior permission of those who appear in the photos or videos
- use another person's account
- post private information about yourself online, including your name, your age, your school name, your address, your phone number, or other identifying information
- use or display the school's name, logo, mascot, or other likeness or representation online which in any way reflects negatively on the school, or Diocese of Wilmington
  This includes, but is not limited to, pictures of anyone wearing clothes with the school name, crest, emblem, or logo. This also includes listing our school name or our employees on a social networking profile, a dating website profile, or a rating website

Use of Personal Electronic Technology Devices (PTD)

PTDs are to be used only when permission has been granted by legitimate authority for educational purposes. Students must set up and use a password on PTDs used in a 1:1 environment.
Students should not:

- use photos, recorded sounds, or recorded images or videos to embarrass or humiliate another person, student or adult
- use devices capable of capturing, transmitting, or storing images or recordings in restrooms, sleeping areas, dressing rooms, or other areas where there is a reasonable expectation of privacy
- alter, change, modify, repair, or reconfigure settings on their own computer or PTD with the intent to hide unacceptable or illegal use of their own devices. This includes deleting cookies and history and re-setting the time and/or date on the computer

Wearable Technology

Because wearable technology is capable of being used to violate this policy and has the potential for being a distraction, teachers have the right to require that students remove wearable technology at any time.

PTDs and Inappropriate Conduct

The content of any PTD can be reviewed by a designated school, parish, or diocesan official as part of any investigation of policy violation or other reasonable suspicion of inappropriate, immoral and/or illegal use. If an illegal act is discovered, local law enforcement officials will be contacted. The Catholic Diocese of Wilmington and its parishes and organizations are not responsible for any harm to PTDs, including but not limited to the loss, theft, damage, or destruction of PTDs or any content therein.

Communication: Social Network and Website Usage, Instant Messaging, Email, Posting, Blog

There are educationally sound exceptions to many of the rules stated in this section. It is up to the local school administration to grant specific exceptions to these rules. Aside from the outright dismissal of these policies, some leeway is allowed.

Teacher and student on line communication must be initiated by the teacher and may take place in the form of an email to students at the beginning of a school year (i.e., when a syllabus and welcome message is sent to students). All teacher/student communication should be educational in nature and not personal.

Students are not permitted to:

- access social networking websites, profiles, or accounts through the school's technology or via PTDs except when directed by legitimate authority for educational purposes
- to upload images to photo-sharing websites without permission from legitimate authority
- access any rating or dating websites through the school's technology or via PTDs access material that is offensive, profane, or obscene including pornography and hate literature
- create social networking pages, accounts, sites, or groups that impersonate or misrepresent teachers or administrators, other students, or other adults in the community
- utilize social networks or website to harass, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community, including adults. This is unacceptable student behavior known as cyberbullying and will not be tolerated. Any cyberbullying, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of the school is subject to disciplinary action
- communicate inappropriately via online posts, whether public or private
- continue communication if another person asks them to stop
- post or send chain letters or spam

Data and Gaming Devices

Unless explicit permission is granted by legitimate authority, students are not allowed to bring gaming devices or other similar data-accessing devices, or personal video game systems onto school property or to school events.

Downloads and File Sharing

- Downloading sound and video files onto school- owned computers is also prohibited. This prohibition applies even if the download is saved to a removable hard drive.
- Students may never configure a school computer or PTD to engage in illegal file sharing. The school will cooperate fully with the appropriate authorities should illegal behavior be conducted by students.
- Students may not download any sound or video files onto their PTD through the school's technology.
- Students may not download any computer game files or attachments from unknown senders.

Intellectual Property, Academic Honesty, Personal Integrity, and Plagiarism

Students should not:

- pretend to be someone else online or use someone else's identity online

- use, post, or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than yourself This includes intellectual property that you were given permission to use personally, but not publically. This behavior violates school policy as well as state and federal laws.
- use resource materials without proper citations.
- utilize some else's work without proper permission
- post, share, or take possession of photos and videos collected as part of an assignment or extra-curricular club, program, or service (i.e., newspaper, yearbook, news channel), with either school owned or PTDs

Filtering

Our school adheres to the requirements set forth by the United States Congress in the Children's Internet Protection Act. This means that all access to the Internet is filtered and monitored. The school cannot monitor every activity, but retains the right to monitor activities that utilize school owned technology. By filtering Internet access, we intend to block offensive, obscene, and inappropriate images and content including pornography.

Responding to Violations of this Policy

Violators of our technology policies will be provided with notice and opportunity to be heard in the manner set forth in the School or Student Handbook, unless an issue is so severe that notice is either not possible or not prudent in the determination of the school administrators. Restrictions may be placed on violator's use of school technologies and privileges related to technology use may be revoked entirely pending any hearing to protect the safety and well-being of our community. Violations may also be subject to discipline of other kinds within the school's discretion. Our school cooperates fully with local, state, and/or federal officials in any investigations related to illegal activities conducted on school property or through school technologies. School authorities have the right to confiscate personally owned technological devices that are in violation or used in violation of school policies.

If you accidentally access inappropriate information or if someone sends you inappropriate information, you should immediately tell a staff member or teacher to indicate that you did not deliberately access inappropriate information.

If you witness someone else either deliberately or accidentally access inappropriate information or use technology in a way that violates this policy, you must report the incident to a school administrator as soon as possible. Failure to do so could result in disciplinary action.

The school retains the right to suspend service, accounts, and access to data, including student files and any other stored data, without notice to the students if it is deemed that a threat exists to the integrity of the school network or other safety concern of the school.

School Liability

The school cannot and does not guarantee that the functions and services provided by and through our technology will be problem free. The school is not responsible for any damages students may suffer, including but not limited to, loss of data or interruptions of service. The school is not responsible for the

accuracy or the quality of the information obtained through school technologies. Although the school filters content, the school is not responsible for student's exposure to "unacceptable" information nor is the school responsible for misinformation. The school is not responsible for financial obligations arising through the use of school technologies.

Right to Update this Policy

Since technology is continually evolving, our school reserves the rights to change, update, and edit its technology policies at any time in order to continually protect the safety and well being of our students and community. To this end, the school may add additional rules, restrictions, and guidelines at any time.

Appendix A - Permission for Student Educational Accounts

Students will be using a variety of online Web applications as a resource to enhance their learning experience. Although these applications are widely used by the education community in K-12 institutions, their Terms of Service state that due to Federal Law any users under the age of 13 must obtain explicit parental permission to use online sites.

All websites and tools that are used commonly in education today have been and will continue to be thoroughly examined by experienced educators. New tools arise every day. Some common tools that your children may encounter and use are, but not limited to:

- Educational Social Networks: A networking site is a place where teachers and students can communicate, collaborate, and share content. Examples include email and cloud file storage and sharing.
- Google Apps: An online suite of productivity and digital tools.
- Electronic Textbooks and Learning Tools/Applications: Information will be provided to the student via electronic text. A multitude of online learning tools will also be used.
- Podcasts and videos: A podcast is a digital audio file that is distributed over the Internet for playback. A video is a recording displaying moving images and audio. Digital video files can incorporate photos, voiceovers and music thus enhancing student research and group projects.

These sites are instrumental in the delivery of the curriculum. We are asking that you and your child please review the permission form below and complete it. Should your expectations change and you wish to revoke your permission, we must be notified in writing. For more information, visit the school website.

Student Information

- Students are responsible for good behavior/character online just like they are in our school building. Students are not permitted to use obscene, profane, threatening, or disrespectful language. Students must notify the teacher of anything inappropriate. Bullying will not be tolerated.
- Copyright infringement occurs when an individual reproduces work without permission that is protected by a copyright. If the user is unsure whether or not to use it, permission is required from the copyright owner.
- All use of these tools must be used in accordance with the Acceptable Use Policy of the Schools and the Catholic Diocese of Wilmington, even if the work is done outside of school on a personal device.

Parent Information

Child Internet Protection Act: The school is required by CIPA to have technology measures and policies in place that protect students from harmful materials including those that are obscene and pornographic. The school is in compliance with CIPA by establishing Internet filters. Any harmful content contained from inappropriate sites will be blocked. http://fcc.gov/cgb/consumerfacts/cipa.html

Children's Online Privacy Protection Act: COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. By default, Google advertising is turned off for Apps for Education users. No personal student information is collected for commercial purposes. This permission

form allows the school to act as an agent for parents in the collection of information within the school context. http://www.ftc.gov/privacy/coppafaqs.shtm

Family Educational Rights and Privacy Act: FERPA protects the privacy of student education records and gives parents the right to review student records. Under FERPA, schools may disclose directory information (name, phone, address, grade level, etc...) but parents may request that the school not disclose this information.

The school will not publish confidential education records (grades, student ID #, etc.) for public viewing on the Internet. The school may publish student work and photos for public viewing but will not publish student last names or other personally identifiable information.

Parents may request that photos, names and general directory information about their children not be published. Parents have the right at any time to investigate the contents of their child's email or web tools. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Appendix B - 1:1 Learning Initiative Agreement

This appendix is provided for schools who have implemented 1:1 learning initiatives.

The focus of a 1:1 Learning Initiative is to provide tools and resources to the 21st century learner. Excellence in education requires that technology be seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. A 1:1 device initiative is a way to empower students to maximize their full potential and to prepare them for college and the workplace. According to studies and school reports, students who use a computing device in a 1:1 educational environment are more organized and engaged learners, attend school more regularly, advance their knowledge and understanding of technology, and become constructors and designers of information and ideas. Learning results from the continuous, dynamic interaction among students, educators, parents, and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning. Effective teaching and learning with 1:1 devices integrates technology into the curriculum anytime, anyplace, anywhere.*

Our Catholic schools provide students with some of the most advanced technology available. Students may be using individual electronic devices (iPads, Chromebooks, tablets, etc.) as determined by their individual school. It is a violation of school policy to use technology for any non-educational use. Unauthorized use, tampering with or destroying equipment, etc., will not be tolerated and will be subject to severe disciplinary action including dismissal. The school's Acceptable Use Policy for Technology has been established by the Catholic Diocese of Wilmington (CDOW) and can be located on the web site (www.cdow.org).

General Guidelines

- Students will have access to all available forms of electronic media and communication that supports the educational goals and objectives of schools in the Catholic Diocese of Wilmington.
- Students will use the devices for educational purposes while at school.
- Students are responsible for the ethical and educational use of technology resources.
- Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to: confidential information, copyrighted material, threatening or obscene material, and device viruses.
- Any attempt to alter data, the configuration of a device, or the files of another user, without the consent of the individual, school administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the Student Code of Conduct.
- Cyberbullying will not be tolerated and appropriate disciplinary action will be taken immediately by the administration.
- Students will use computers/devices in a responsible and ethical manner.
- Students may only sign on to the designated network.
- Students must set up and use a password to access the device.
- Students may not add or delete settings or apps that allow the student to bypass Internet filtering on the device.
  Students are expected to obey general school rules concerning behavior and communication that apply to network use in accordance with the Catholic Diocese of Wilmington Acceptable Use Policy. This policy is available online and must be signed by students and their parents each year as part of the student registration.
- Students are expected to use all technology resources in an appropriate manner so as not to damage school

equipment. This "damage" includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by the student's own negligence, errors or omissions. Use of any information obtained via the school's designated Internet system is at the student's own risk. The Catholic Diocese of Wilmington and the school specifically deny any responsibility for the accuracy or quality of information obtained through its services.

- Students are expected to assist the Catholic Diocese of Wilmington and the school to protect the computer system/device by contacting an administrator about any security problems they may encounter.
- Students are expected to monitor all activity on their account(s).
- Students should always turn off and secure their device after they are done working to protect their data and privacy.

Privacy and Safety

- Unauthorized chat rooms and all chain letters are prohibited.
- Students may not open, use or change device or files that do not belong to them.
- Students may not reveal their full name, phone number, home address, social security number, credit card numbers, password or passwords of other people without the permission of their parent.
- Students must remember that the information stored on their device is not guaranteed to be private or confidential.
- If a student inadvertently accesses a website that contains obscene, pornographic, or otherwise offensive material, the student must notify a teacher or an administrator immediately so that such sites can be blocked. This is not a request – it is a responsibility.
- Student use of the Internet on the school's network is filtered per local policy, as required by state and federal mandates.
- If a student should receive email or other electronic messages containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to document evidence and report to legitimate authority.

Parent Responsibilities:

- Talk to your child about values and set standards regarding the use of the Internet, just as you do on the use of all media information sources such as television, telephones, movies, and radio.
- Attend orientation: Parents/guardians are required to attend the 1:1 Orientation, comply with the policies set forth in this document and the AUP, and sign the AUP.
- Monitor device use: Parents/guardians are required to monitor personal use of devices outside of school to ensure compliance with school policies. Potentially dangerous sites are blocked with the school's filter while devices are logged on to the school network. Outside of school, parents may want to monitor or restrict their home Internet access.
- Monitor purchases: It is the parent's responsibility to monitor all purchases.

Student responsibilities:

- Attend orientation: Students are required to attend the 1:1 Orientation, comply with the policies set forth in this document and the AUP, and sign the AUP.
- Care for and use of the device at school: Students must have their devices available for all classes. Devices are intended for use at school each day; however, using the device is viewed as a privilege, not a right. Students must use their devices in a responsible and ethical manner, abide by all guidelines and policies set forth in this document and the AUP, obey general school rules, and respect the request of legitimate authority with regard to the use of the device. Students must not share their device or account information with peers.

- Charge device battery: Students must fully charge their devices battery prior to each school day. Charging devices during school hours is not an option, as electrical outlets are sparse. Coming to school with a device that is not charged will result in appropriate disciplinary action, as well as academic consequences.
- Manage files and save work: In addition to saving work as directed by the teacher, students may wish to create their own backups. It is the student's' responsibility to ensure that all work is saved appropriately. Students are academically responsible for all work, despite technical failures or accidental deletions.

*Adrian Public Schools, Adrian, MI

Resource One - Definition and Terms

Bandwidth – Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time.

Cyberbullying - Cyberbullying is sending derogatory or threatening messages and/or images through a technological medium in an effort to ridicule or demean another. Cyberbullying also takes place when someone purposefully excludes someone else online or when someone creates a fake account or website criticizing or making fun of another.

Internet – The Internet connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.

Legitimate Authority - A school, parish, or diocesan employee with the authority to grant explicit permission for specific actions as defined by leadership.

Minor – Anyone under the age of 18 years of age or still attending high school.

Network – The school's network is defined as our computers and electronic devices such as printers, fax machines, scanners, etc. that are connected to each other for the purpose of communication and data sharing.

Personal Technology Device User – For the purposes of this policy, personal technology device user refers to anyone who utilizes their own technology on property owned or controlled by the school or at a school sponsored event.

Personal Technology Device (PTD) - A personal technology device is any device owned by a student or his/her parents or guardians.

Social Media - Social media are works of user-created video, audio, text or multimedia that are published and shared in a social environment, such as a blog, wiki or video hosting site.

Technology – Under this policy, technology is a comprehensive term including, but not limited to, all computers, projectors, televisions, DVD players, stereo or sound systems, digital media players, gaming consoles, gaming devices, cell phones, personal digital assistants, CDs, DVDs, camcorders, calculators, scanners, printers, cameras, external and/or portable hard drives, modems, Ethernet cables, servers, wireless cards, routers and the Internet. *School technology* refers to all technology owned and/or operated by the school. This includes Internet access, computers, printers, etc.

User – For the purposes of this policy, user is an inclusive term meaning anyone who utilizes or attempts to utilize, whether by hardware and/or software, technology owned by the school. This includes students, faculty members, staff members, parents, and any visitors to the campus.

Wearable Technology - Wearable technology is a group of devices that can be worn by individuals that has the ability to track data related to the individual that wears it. It contains sensors that detect motion, external conditions, take video, sound, and photos, send and receive data, and communicate all this information in real time for the user to access on the device or multiple other devices.

Appendix C - Signature Page

Only one student agreement per family is required.

I have read, understand, and agree to follow all rules, regulations, and policies as outlined in the Acceptable Use of Technology Policy. Should I commit any violation of the policy, I understand and agree that my access privileges may be revoked and discipline action and/or legal action may be taken.

Signature of Student	Date	Grade Level

Please Print Name

I agree to waive any claim against the Catholic Diocese of Wilmington, its organizations and institutions ("CDOW"), and release CDOW from any liability for any violation of the terms of the agreement and further agree to indemnify and hold harmless CDOW from any third party claims which may result from violating the terms of the agreement, including but not limited to all attorney fees and court costs which may arise from said violation.

Signature of Parent/Guardian	Date

Please Print Name	Date