Diocese of Wilmington
Catholic Schools
Acceptable Use of Technology
Student Edition

Instructions

The Catholic Schools Office, Catholic Youth Ministry and the Office of Religious Education have partnered with Campus Outreach Services to develop comprehensive policies regarding the use of technology in elementary, high schools and for employees. This document is the policy for students enrolled in schools in the Diocese of Wilmington. It is to be inserted within a new section of each school's student policy handbooks. This new section should be named "Acceptable Use of Technology." These policies may not be edited.

All schools are required to review student policies with students and faculty/staff annually before allowing students initial network access or beginning computer classes. Documentation of how this is accomplished must be provided to the school principal and kept on file for the remainder of the school year. (For example, a teacher may review all policies during the first week of school and document this instruction via their lesson plans or an assignment in PowerTeacher Gradebook™.)

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 cyber-bullying awareness and response.

rev. 05/14/12

Acceptable Use of Technology

Table of Contents

Introduction

Access to technology is integral to the educational mission and purpose of our institution. We utilize technology in nearly every facet of instruction, activity, service, research, and operation of our school. 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 limited educational purposes, not as a public access service.

Due to the evolutionary nature of technology, it is imperative for students to realize that our policies regarding the use of technology in our community will also be evolutionary. We ask all students to employ their best judgment when it comes to the use of school technology and keep in mind that our policies related to technology are not meant to supersede our other school policies, but rather to complement them. Although our school provides certain technologies, we recognize that members and guests of our community also have their own technology devices that they bring to our campus and school events. Our policies address the appropriate use of both technologies provided by the school and personally owned technological devices. 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.

No policy can detail all possible examples of unacceptable behavior related to technology use. Our school technology users are expected to understand that the same rules, guidelines, and policies that apply to non-technology related student behavior also apply to technology-related student behavior. Our school technology users are expected to use their best judgment when it comes to making decisions related to the use of all technology and the Internet. If there is ever an issue about which you are unsure, seek the advice of legitimate authority.

This Policy applies only 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.

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.

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.

Legitimate Authority

Throughout this document, the term "legitimate authority" is used. Legitimate authority indicates a school, parish, or diocesan employee with the authority to grant explicit permission for specific actions (i.e., a teacher may give permission for a student to use the Internet during class but another student does not have the legitimate authority to grant such permission). It is up to individual institutions to define and limit "legitimate authority" (i.e., a teacher may have permission to allow students on the Internet during class, but such permission does not assume he/she may allow young people to override school policies and permit use of social networking sites or video games).

Personal Responsibility

We expect our students to act responsibly and thoughtfully when it comes to using technology. 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 other school administrator 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. Educational purposes include classroom activities, career development, and communication with experts, homework, and limited high quality self- discovery activities. Commercial 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 the educational purposes stated above. The school is not responsible for any damages, injuries, and claims resulting from violations of responsible use of technology.

Privacy

All communication that takes place using personally owned or school owned technology must reflect the mission and values of the school and the Catholic Diocese of Wilmington. This includes emails, texts, instant messages, and posts online. Your attendance at this school acknowledges your commitment to upholding the values and mission taught in this institution.

Students should not expect that what they write or publish online is private. As such, 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 onto a school computer can also be inspected. Students have a limited expectation of privacy when using their own technology on school property or at school events so 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

Network storage is a finite school resource and we expect students to be respectful of other users and limit the amount of space and memory taken up on school computers and on the school network.

Any student (those provided with a school email account and those who are not provided such an account) must understand that all emails and messages sent from this account or via a school network are representative of the school and must reflect the mission and values taught here. Electronic communication by students must be in accord with school policies regarding appropriate language use, bullying, stalking, and other policies and laws. Student email accounts are subject to monitoring and have limited privacy. Students should be aware sharing resources such as bandwidth and

server space with others and downloading large files utilizes finite resources. Abusing these resources can result in the loss of this privilege. Please delete old emails and save large attachments elsewhere to limit the amount of storage space used.

The Diocese of Wilmington requires that any schools with wireless Internet access must protect Internet connections with a password. Connection to wireless Internet by students is prohibited unless otherwise directed/instructed by legitimate authority.

Only IT personnel may connect computers and devices to the school's Ethernet ports and disconnect computers and devices currently connected to the school's network.

The school provides individual technology accounts for students to keep track of their technology use. Users must log off when they are finished using a school computer. Failing to log off may allow others to use your account, and students are responsible for any activity that occurs through their personal account.

Termination of Accounts and Access

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

Our school is a community and as such, community members must respect the privacy of others. Do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others. Do not misrepresent or assume the identity of others. Do not re-post information that was sent to you privately without the permission of the person who sent you the information. Do not post private information about another person. Do not post photos or videos of others without prior permission of those who appear in the photos or videos. Do not use another person's account. If you have been given an account with special privileges, do not use that account outside of the terms with which you were given access to that account.

Except as required for educational purposes, do not voluntarily post private information about yourself online, including your name, your age, your school name, your address, your phone number, or other identifying information.

Our institution prides itself on its reputation for excellence; therefore, you may not use the school's name, logo, mascot or other likeness or representation on a non-school website in a manner than compromises the mission and values of the school or Catholic Diocese of Wilmington. This includes 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 such as RateMyTeacher.com or RateMyCoach.com.

Personal Boundaries

Students should respect the personal and professional boundaries of other students and of teachers. Therefore, it is not acceptable for young people to initiate electronic communication with teachers, adult leaders in ministry, or administrators. Because parental permission is required for communication between a young person and Church Personnel, the adult leaders in ministry must initiate communication. Required initiation of communication 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).

In all cases, the privacy of the student and appropriate boundaries are paramount.

Use of Personal Electronic Technology Devices (PTD)

All extraneous personally owned technology devices (PTD), including, but not limited to, cellular phones, BlackBerrys, pagers, beepers, gaming devices, headsets, tablet PCs, mobile presenters, wireless tablets, digital audio and video recorders, Palms, Sidekicks, iPods, Kindles, iPads, MP3 players, texting calculators, camera video phones, digital cameras or laptops are to be used only when permission has been granted by legitimate authority for educational purposes. This includes devices that are run using commercially available networks (i.e., AT&T, Verizon, Sprint, etc.).

During a period of heightened security or an actual lock down of a school or campus, care must be given not to compromise the instructions of emergency or school personnel (i.e., common sense dictates that parents would naturally begin trying to reach their children (and vice versa) during an emergency but every effort must be made to limit communication so that instructions are clear and consistent).

Young people may not use photos, recorded sounds, or recorded images or videos in such a manner as to embarrass or humiliate another person, student or adult. Devices capable of capturing, transmitting, or storing images or recordings may never be accessed or operated in restrooms, sleeping areas, dressing rooms, or other areas where there is a reasonable expectation of privacy.

To protect the safety and well-being of students', staffs' and other community members' personal property and to avoid disruptions to the learning environment; group leaders, teachers, or school personnel reserve the right to confiscate or collect any PTD.

The content of any PTD device may be reviewed by a designated school or parish official as part of any investigation of policy violation or other suspected 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 by not limited to the loss, theft, damage, or destruction of PTDs or any contents therein.

Social Network and Website Usage

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.

Social networking websites, profiles, or accounts, may only be accessed through the school's technology or via personally owned technology devices when directed by legitimate authority for educational purposes.

Because the terms of service of most photography sharing websites transfers ownership of uploaded images from the individual (or school) to the website itself, extreme caution must be taken when accessing any photography sharing websites including, but not limited to, Photo Bucket, Webshots, Flickr, and Fotki. If the terms of service indicate such a transfer of ownership (i.e., the website can do as they wish with the photos), such websites must not be used, even for educational purposes.

Students are not permitted to access through the school's technology or via personally owned technology devices accessed via commercially available networks (i.e., AT&T, Verizon, etc.) any rating or dating websites including, but not limited to, RateMyTeacher.com, RateMyCoach.com, or JuicyCampus.com.

Students may not access material that is offensive, profane, or obscene including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity, nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

Students are not permitted to access from the school's technology any instant messenger services including, but not limited to, AOL, AIM, Skype, Yahoo! Messenger, MSN Messenger, and Gtalk.

It is not acceptable for students to create social networking pages, accounts, sites, or groups that impersonate or misrepresent teachers or administrators, other students, or other adults in the community. Students may not 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 cyber-bullying and will not be tolerated. Any cyber-bullying, on or off-campus, that is determined to substantially disrupt the safety and/or well being of the school is subject to disciplinary action.

Communication: Instant Messaging, Email, Posting, Blog

Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students. Inappropriate communication includes, but is not limited to the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by students; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If you are told by another person to stop sending communications, you must stop.

Students may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy any individual. This is unacceptable student behavior known as cyber-bullying and will not be tolerated. Any cyber-bullying, on or off-campus, that is determined to substantially disrupt the safety and/or well being of the school is subject to disciplinary action.

Do not post or send chain letters or spam. Spamming is sending an unnecessary and unsolicited message to a large group of people. Spamming occurs through email, instant messages, or a text messages.

Data and Gaming Devices

Unless explicit permission is granted by legitimate authority, students are not allowed to bring iPods, MP3 players, CD players, DVD players, or other similar data-accessing devices, or personal video game systems onto school property or to school events.

Unless legitimate authority grants explicit permission, students may not use the school's technology to play computer games.

International Websites

Because foreign language websites cannot be filtered using our current system, these websites may only be accessed from school owned technology under the direction of legitimate authority.

Downloads and File Sharing

Students may never download, add, or install new programs, software, or hardware onto school-owned computers. 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 their school computer or personally owned technology device to engage in illegal file sharing. The school will cooperate fully with the appropriate authorities should illegal behavior be conducted by students.

The likelihood of accidentally downloading a virus or spyware when downloading music and movies is very high; therefore students may not download any sound or video files onto their personally-owned technological devices through the school's technology. Students also may not download any computer game files or attachments from unknown senders.

Intellectual Property, Academic Honesty, Personal Integrity, and Plagiarism

All students are expected to maintain academic honesty. Do not claim or imply that someone else's work, image, text, music, or video is your own. This is plagiarism and will not be tolerated. Plagiarism is also when you incorporate a piece of someone else's work into your own without giving them appropriate credit. Do not pretend to be someone else online or use someone else's identity without express permission from that person and/or his/her parent/guardian if he/she is a minor. Do not 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.

A work or item is copyrighted when, among other issues, one person or one group owns the exclusive right to reproduce the work or item. Songs, videos, pictures, images, and documents can all be copyrighted. Copyright infringement is when you violate copyright law and use or reproduce something without the authority to do so. Make sure to appropriately cite all materials used in your work. Do not utilize some else's work without proper permission.

If students take photos or videos as part of an assignment or an extra-curricular club, program, or service (i.e., newspaper, yearbook, news channel), with either school owned or personally owned technology devices; those photos and videos are the property of the school, not the individual. Therefore, students may not post, share, or take possession of photos and videos collected.

Commercial and Political Use

Commercial use of school technology is prohibited. Students may not use school technology to sell, purchase, or barter any products or services. Students may not resell their network resources to others, included, but not limited to, disk storage space. The school is not responsible for any damages, injuries, and/or claims resulting from violations of responsible use of technology. Students who are engaged in fund-raising campaigns for school sponsored events and causes must seek permission from legitimate authority before using technology resources to solicit funds for their event.

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.

Computer Settings and Computer Labs

Unless legitimate authority grants explicit permission, students are not allowed to alter, change, modify, repair, or reconfigure settings on school-owned computers. This includes deleting cookies and history and re-setting the time and/or date on the computer.

Students are not permitted to alter, change, modify, repair, or reconfigure settings on their own computer or other technology device 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.

Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited.

Unless legitimate authority grants explicit permission, food and drink are prohibited from school computer labs. Students may not eat or drink while using any school- owned computers or other technologies.

Students may not circumvent any system security measures. The use of websites to tunnel around firewalls and filtering software is expressly prohibited. The use of websites to anonymize the user is also prohibited. The use of websites, both domestic and international, to circumvent any school policy is prohibited. Students may not alter the settings on a computer in such a way that the virus protection software would be disabled. Students are not to try to guess passwords. Students may not simultaneously log in to more than one computer with one account. Students are not to access any secured files, resources, or administrative areas of the school network without express permission or the proper authority.

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 so as to prove 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 obtained through school technologies <if you do filter, use this>), 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.

Resource One

Definition and Terms

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

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

<u>Internet</u> – 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.

<u>Legitimate Authority</u> - A school, parish, or diocesan employee with the authority to grant explicit permission for specific actions.

<u>Minor</u> – Anyone under the age of 18 years of age or still attending high school.

<u>Network</u> – 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.

<u>Personally Owned Device/User</u> – For the purposes of this policy, personally owned device user refers to anyone who utilizes their own technology on property owned or controlled by the school or at a school sponsored event. A personally owned technological device is any device owned by a student or his/her parents or guardians.

<u>Social Media</u> - 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.

<u>Technology</u> – 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.

<u>User</u> – 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.

Resource Two

General Safety Tips

Posting Online and Social Networking: These guidelines prohibit young people from accessing social media sites except when instructed to do so in the course of an educational activity. When at home, be sure to follow these guidelines.

- Most social networking sites have an age requirement; make sure you follow that requirement.
- Never post personal information about yourself online. Personal information includes your phone number, address, full name, siblings' names, and parents' names.
- When creating an account on a social networking website, make sure to set your privacy settings so only your friends can view your pictures and your profile.
- Avoid accepting a friend you do not already know.
- If possible, set up your account so that you are notified of any postings onto your wall or page.
- Set up your account so that you have to approve all postings to your wall or page.
- Set up your account to notify you when someone else has posted and tagged you in a picture.
- If you have a public profile, be careful about posting anything identifiable such as a sports team number or local park where you spend your free time.
- In general, do not post pictures of friends or other young people (or adults) without the expressed permission of those in the photos/videos.

Communications: Think before you send all forms of communication, including emails, IM's, and text messages. Once you send the data it is not retrievable, and those who receive it may make it public or send it along to others, despite your intentions.

Strangers: Do not feel bad about ignoring instant messages or emails from unknown people. Save all contacts from known or unknown people who are repeatedly contacting or harassing you. These saved messages will help authorities track, locate, and prosecute cyber-stalkers and cyber-bullies.

Passwords: Do not share your passwords with your friends. When creating a password, do not make it anything obvious such as your pet's name or favorite sports team. Also remember to include both letters and numbers in your password if possible.
Downloads and Attachments: Do not open or run files on your computer from unknown or suspect senders and sources. Many viruses and other undesirable consequences can result from opening these items.

Stay Current: Do protect your own computer and devices by keeping antivirus and antispyware up to date. Keep your operating system and application software up to date. Turn off file sharing as an option on your computer.

Remember that once words are published online, those words are online forever. Think before you post, send, or text.