Acceptable Use of Technology in Ministry

An Addendum to Ethical Standards for Church Personnel

Catholic Diocese of Wilmington

July, 2016

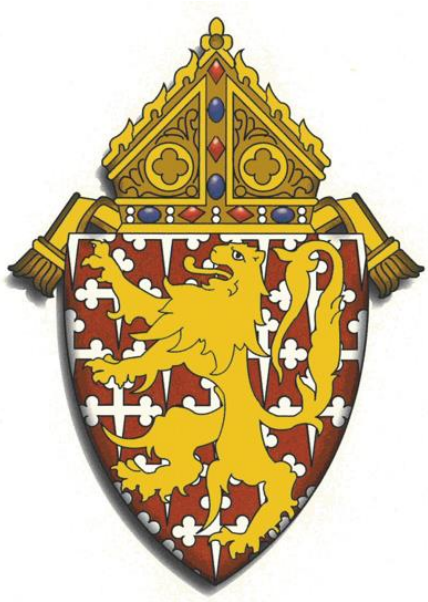

Table of Contents

Section One – Technology-Related Standards of Conduct

This Acceptable Use Agreement applies to all Church Personnel and any individual or organization, including, but not limited to, Alumni Associations, Athletic Associations, Scouting, Knights of Columbus and any other individual, group, or organization who have been granted permission by the appropriate legitimate authority to use employer-owned technology and/or have been granted permission to create social media accounts using the intellectual property of the Diocese of Wilmington, schools, or parishes.

Users agree that this Acceptable Use Agreement will be reviewed and signed annually.

The use of all employer-owned technology and the use of personally owned technology devices on diocesan, parish, or school grounds or at employer-sponsored events is a privilege not a right.

Supervision

All parishes and schools must have one person on staff designated as the "legitimate authority" when it comes to granting permission for the use of employer-owned technology. This person should have a general knowledge of technology and how it can be used in ministry.

Who Can Use Technology?

Only Church Personnel are permitted to use employer-owned technology resources, unless prior approval is obtained from the legitimate authority. Church Personnel are responsible for unauthorized use of their technology account, including access by children, spouses, or significant others.

Personal use of employer-owned technology is permissible only with the express permission of the legitimate authority. Church Personnel bear the burden of responsibility to inquire with the IT Department (in the case of schools) or other legitimate authority when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

Privacy

The employer reserves the right to monitor and track all behaviors and interactions that take place online or through the use of technology on employer property or at employer-related events. This includes emails, texts, and document or image files. The employer reserves the right to investigate any reports of inappropriate actions related to any technology used while serving as Church Personnel.

Church Personnel have a limited expectation of privacy when using their own technology on diocesan, parish, and school property, as long as no activity violates this policy, law and/or compromises the safety and well-being of participants.

Purposes and Expectations of Use for Technology

The use of all employer-owned technologies is limited to ministry purposes.

Section Two – Parental Permission

Obtaining Parental Permission

For ministry purposes, permission of the parent or guardian must be obtained, annually, in writing, in order for Church Personnel to:

- communicate electronically with minors
- share/post pictures or videos of minors
- share email, telephone numbers, or other contact information with other minors or adults who are part of the class, group or organization (i.e., in the case of a parish Confirmation class, or retreat experience, for instance)

Suggested language can be found in ***For the Sake of God's Children*** Form A.

Section Three – Personal Devices

Personal Technology Device (PTD) Defined

PTDs include, but are not limited to, any electronic device capable of communication, and/or capturing and transmitting images, sound or signals.

Acceptable Use of Personal Technology Devices (PTDs)

- Those who work with young people in parishes and schools have a duty to be aware of the role they play in providing a safe environment for young people.
- The personal use of PTDs is limited to those times when Church Personnel are not actively engaged in the supervision of young people.
- The use of a PTD is permissible in cases of emergency (as directed by emergency personnel) or when used as part of an activity or event.

PTDs Used on Employer's Network

- Personal computers, when used on employer's network, must have up-to-date antivirus software installed and browser preferences set appropriately.
- Church Personnel may not download any sound or video files onto their personal technology devices through the employer's network, except when legally used for educational purposes.

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.

Confiscating and/or Searching PTDs Belonging to Minors

The Supreme Court of the United States has determined that a search of a PTD is, by its nature, more "intrusive" than the search of a backpack, purse, or other physical space.

If a PTD is found and its ownership is unclear, the PTD should be turned into the legitimate authority located in the principal office of the facility. It is not acceptable to search the PTD for ownership except under emergency threat situations.

Once a PTD is in the possession of legitimate authority, a search should only occur if the PTD is reasonably suspected to contain materials that pose a threat. Materials on a PTD that might pose a threat include, but are not limited to, evidence of obscene or harmful content, illegal activity, harassment, and/or security threats.

In cases other than emergency situations and for the protection of the student and Church Personnel, any search should be done in consultation with, and, if possible, in the presence of, the parents of the young person.

Section Four – Internet and Electronic Communication

All Church Personnel, regardless of the role they play in ministering to the faithful, are bound by the following:

Overview

- It is not acceptable for Church Personnel to engage in the repeated, persistent monitoring and/or patrolling of online activity of the young people to whom they minister without legitimate reason.
- Church Personnel should never consider electronic communication (emails, social networking sites, text message, etc.) to be private and should not be used to address/discuss confidential matters.
- Church Personnel should address and model online safety with minors when used as part of their program.

Email

- Use an email account on a device that is protected by anti-virus software.
- Do not communicate with minors to whom you minister using your personal email address.
- Do not share a minor's email address with others without prior permission of parents or guardians.
- Save copies (either printed or electronically) of all communications with minors for a period of five years.
- Report any violation of this policy to the appropriate supervisor.

Online Video and Chat

Parent/guardian permission is required for ministry-related online video and/or chat sessions between Church Personnel and minors. Church Personnel must obtain permission from an appropriate legitimate authority to initiate and/or engage in ministry-related online video and/or chat sessions with minors.

Text Messaging

Because one-on-one text messaging between Church Personnel and minors is not appropriate, when using Mobile Text Data (Texting) and Short Messaging Service (SMS), Church Personnel must adhere to the following:

- When communicating with minors mass-texting services must be used.
- Church Personnel should not respond to inappropriate or personal text messages from minors to whom they minister and are required to inform the appropriate legitimate authority.

Blogs and Microblogs

- Blogs used for educational or ministerial purposes must be approved by the appropriate legitimate authority and the content should reflect the purpose. Access by the legitimate authority is a condition of approval.
- The owner of the blog must be diligent in monitoring for inappropriate activity.
- Personal blogs should not be intentionally shared with minors.

Social Media

Ministry Use

- The appropriate legitimate authority must give permission for Church Personnel to establish a social networking site related to the parish, school or organization.

- Parishes and schools must comply with social media policy age restrictions.
- Appropriate privacy settings must be used and regularly audited.
- Permission to post from the social media account must be granted by the appropriate legitimate authority.
- A social media account should only be used as a virtual billboard to post details of school or parish events, and must not be used as a means of one-on-one communication. Digital relationships which link to other accounts must be specifically related to ministry purposes.
- Images or videos of minors or events may only be posted on a ministry online account if those in the images or videos grant specific permission. Church Personnel must comply with requests from a parent that images or videos be removed.
- Non-public personal information must not be posted.

Private Use

- Volunteers, who are not otherwise defined as Church Personnel, may not communicate with minors via social media without written permission of a parent or guardian.
- Church Personnel who use social networking sites to communicate with minors about their ministry must use an account registered in the name of the parish, school, or diocese.

Direct Messaging

Any services that include the ability for direct messaging are subject to all of the rules stated herein.

Photographs and Audio, Video Recording

- Devices capable of capturing, transmitting, or storing images or recordings may never be accessed or operated in restrooms, dressing rooms, sleeping areas, or other areas where there is a reasonable expectation of privacy.

- Audio and/or video recordings are not permitted without the expressed consent of those being recorded.

Commercial and Political Use

- Church Personnel may not use employer-owned technology to sell, purchase, or barter any products or services for personal gain. Church Personnel who are engaged in fund-raising campaigns for parish or school-sponsored events and causes must seek permission from their supervisor before using employer-owned technology resources to solicit funds for their event.

- Political use of employer-owned technology is prohibited without prior, specific permission from appropriate legitimate authority (as in the case of a letter writing campaign supporting specific funding for schools or opposing legislations that is contradicted by our Catholic faith).

Use of Logos and Mascots

Church Personnel may not use or display the parish or school's name, logo, mascot, or other likeness or representation online which in any way reflects negatively on the parish, school, or Diocese of Wilmington.

Section Five – School Specific Policies

This section includes specific mandates for Catholic Schools in the Diocese of Wilmington.

Filtering

Schools must adhere to the requirements set forth by the United States Congress in the Children's Internet Protection Act that all access to the Internet is filtered and monitored.

School Provided Technology

- Where wireless Internet is provided, it must be protected by a password. To access wifi, contact a member of the Technology Department. Unauthorized access is forbidden.
- Users must log off when they are finished using a computer to avoid unauthorized use of their account. Schools are not responsible for any activity that occurs through a personal account.
- Employees are responsible for unauthorized use of their technology account.
- Unless required for educational purposes, foreign language websites cannot be accessed using school technology (since such sites are often impossible to block using English language based filters). Exceptions may be granted on a case-by-case basis by the appropriate legitimate authority.

Download and File Sharing

Unless permission is granted by the IT Department or school administration, school personnel may never download, add, or install new programs, software, hardware or sound and video files onto school-owned computers and removable hard drives.

Computer Settings

School personnel 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 make a user anonymous is also prohibited.
- The use of websites, both domestic and international, to circumvent any diocesan, parish, or school policy is prohibited.
- School personnel may not alter the settings on a computer in such a way that the virus protection software would be disabled.
- School personnel are not to access any secured files, resources, or administrative areas of the employer network without express permission of the proper authority.
- School personnel may not alter, change, modify, repair, or reconfigure settings on school-owned computers without the permission of the appropriate legitimate authority.
- No alterations may be made to hide unacceptable or illegal use.

Section Six – Prohibited Online Activity

Church Personnel may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy any individual. Any behavior, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of others is subject to investigation. This includes, but is not limited to:

- Posting or accessing pornography or other offensive legal or illegal material, including hate literature, defamatory, libelous, offensive or demeaning material
- Engaging in inappropriate behavior, including but not limited to engaging minors in sexual dialogue or sending inappropriate pictures to minors
- Disclosing confidential information of any kind
- Discussing or showing pictures of minors online in an inappropriate manner
- Engaging with any minor in a way which could be considered a peer-to-peer communication
- Accessing from employer-owned technology any rating or dating websites
- Sending chain letters or spam

- Playing computer games on employer-owned computers, unless part of an academic exercise or officially sanctioned event (i.e., a class, religious education class, or youth ministry event)
- Purposefully spreading or facilitating the spread of a computer virus
- Downloading or installing new programs, software, or hardware onto employer-owned computers with the exception of routine software updates, and without expressed permission of legitimate authority
- Illegally downloading sound and video files or engaging in illegal file sharing on employer-owned computer or networks
- Accessing social networking sites from PTDs while actively serving as a supervisor for young people
- Claiming or implying that someone else's work, image, text, music, or video is your own
- Pretending to be someone else online or using someone else's identity

Section Seven – Violations and Liability

School Personnel who violate technology policies will be provided with notice and opportunity to be heard in the manner set forth in the Employee/Faculty Handbook, unless an issue is so severe that notice is either not possible or not prudent by the determination of the employer or its administrators.

Church Personnel may be terminated from paid or volunteer positions should their online activities reveal behaviors that are inconsistent with civil law and/or the teachings of the Catholic Church.

The Diocese of Wilmington and its organizations and institutions will cooperate fully with local, state, and/or federal officials in any investigations related to illegal activities conducted on parish property or through parish technologies.

If inappropriate information is accessed or sent to you, you should immediately tell a supervisor or other legitimate authority so as to prove you did not deliberately access inappropriate information.

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

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

Liability

The employer cannot and does not guarantee that the functions and services provided by and through technology will be problem free. The employer is not responsible for any damages Church Personnel may suffer, including but not limited to, loss of data or interruptions of service. The employer is not responsible for the accuracy or the quality of the information obtained through parish technologies. The employer is not responsible for one's exposure to "unacceptable" information, nor is the employer responsible for misinformation. The employer is not responsible for financial obligations arising through the use of employer technologies.

The employer is not responsible for any damages, injuries, and/or claims resulting from violations of responsible use of technology.

Section Eight – Glossary of Terms

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

Blogs – Blogs are web logs, which are public and can be accessed by anyone. Blogs are used to share information, educate, or express opinions.

Microblogs – Microblogs can accomplish the same goals but restrict the size of the message for direct and simple communication.

Cyberbullying - Cyberbullying refers to the use of a technological medium to send derogatory or threatening messages and/or images in an effort to ridicule or demean another. Cyberbullying includes when someone purposefully excludes someone else online, and when someone creates a fake account or website criticizing or making fun of another, also known as social exclusion.

Church Personnel - As outlined in ***For the Sake of God's Children***, the following are included in the definition of Church Personnel**.**

The Bishop and all who share in his ministry:

- Priests incardinated in the Diocese of Wilmington
- Priests who are members of Religious communities (e.g. Oblates, Franciscans, Jesuits etc.) assigned to the Diocese
- Priests of other jurisdictions who minister within the Diocese; retired priests, or others who have been granted canonical faculties to do part-time or supply ministry
- Deacons incardinated in this Diocese; permanent deacons with canonical faculties to function in this Diocese and those retired and living in the Diocese
- Seminarians, those enrolled in the Permanent Diaconate Formation Program, and those in the formation programs of religious congregations
- Men and women Religious working and living in the Diocese, its parishes, schools or agencies; living in the Diocese of Wilmington and working elsewhere; working in the Diocese but living elsewhere; and retired and living in the Diocese of Wilmington
- All paid personnel whether employed in areas of ministry or other kinds of services provided by the Diocese, its parishes, schools or other agencies
- All volunteers including any person who enters into or offers himself/herself for a Church-related service

Direct Messaging - Direct messaging refers to a feature of certain social media applications which permit non-public messages to be exchanged between users.

Employer - The term "employer", for the purposes of this document, refers to any parish, school, office, or department of the Catholic Diocese of Wilmington.

Employer-owned Technology - Employer-owned technology refers to all technology owned and/or operated by the employer. This includes, but is not limited to, Internet access, computers, printers, and the information contained therein.

Hate Literature - Hate literature includes 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).

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 - The term "legitimate authority" refers to a school, parish, or diocesan employee with the authority to grant explicit permission for specific actions. "Appropriate legitimate authority" refers to the specific school, parish, or diocesan employee who, in a specific situation, has such authority.

Mass Texting Services - Mass texting services are software applications (e.g. Remind) which permit the user to send text messages out to subscribers without direct access to subscriber cell phone numbers. It is commonly used for alerts and reminders.

Ministry Purposes – Ministry purposes shall be defined by the employer, subject to the terms of an employment agreement where applicable.

Minor – A minor is anyone under the age of 18 or who is still a registered student at a high school or in parish youth ministry/religious education activities in the Diocese of Wilmington.

Network – The school, parish, or diocesan network is defined as 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.

Non-Public Personal Information - Non-public personal information is any data or information considered to be personal in nature and not subject to public availability including, but not limited to, personal email addresses, private cell phone numbers, and personal social media accounts.

Personal Device/User – For the purposes of this policy, personal device user refers to anyone who utilizes their own technology on property owned or controlled by a school, parish or the diocese or at a school, parish or diocesan-sponsored event. A personal technological device is any device owned by a student, faculty member, staff member, parent or guardian, or visitor.

Sexting - Sexting is the act of electronically sending sexually explicit messages, images, or video.

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.

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 schools, parishes or the diocese. This includes students, faculty members, staff members, parents or guardians, volunteers, and visitors.

Virtual – For the purposes of this policy, virtual refers to technology used outside the presence of gathered, face-to-face experiences; not physically present but made by software to appear to be present.

Volunteer - A volunteer is a person who freely offers to take part in a Church ministry or undertake a task without monetary compensation. In the Diocese of Wilmington, this can include parents who volunteer and have regular recurring contact with children five (5) hours or more within a year and are required to sign a Volunteer Covenant and participate in the ***For the Sake of God's Children*** training.

Appendix A: Technology Best Practices

This is a set of guidelines of best practices for Church Personnel and how they interact with each other and the wider community online.

The Golden Rule of Technology

The best rule when communicating online is "when in doubt, don't post (or send or publish, etc.)." There is no effective way to erase digital content.

Internet Access and Computer Usage

- If diocesan or parish offices utilize a server to manage Internet connectivity, a filter should be in place to monitor all access to the Internet.
- All computers with Internet access should have antivirus software installed, and should be scanned for viruses and updated regularly.
- If wireless Internet is provided, it should be protected by a password.
- Users should log off when they finish using a computer. Failing to log off may allow others to use an account, and Church Personnel would bear responsibility for any misuse on individual accounts that results.

Email

- Protect the privacy of others by using the “blind carbon copy” (BCC) protocol when sending to more than one recipient.
- Maintain a separate email address for professional communications and personal communication.
- Professional communication should avoid abbreviations and use proper spelling, grammar and punctuation.
- Exercise discretion when using “Reply All” feature even if others in the communication thread have done so.

Archiving Electronic Communication

In 2006, the U.S. Supreme Court's amendments to the Federal Rules of Civil Procedure created a category for electronic records that explicitly named emails and instant message chats as records to be archived and produced when relevant. This means that if a school, parish, or diocese is sued, any electronic communications are discoverable within the litigation process.

Parishes, Schools, and Diocesan organizations should follow these guidelines:

- Communication between young people and Church Personnel should be archived for a period of at least five years.
- All communication between a parent and teacher regarding the progress or discipline of a student should be archived for a period of at least five years.
- After a period of five years, any emails should be purged so long as above policies have been followed and there is no active litigation.

It is the responsibility of local parishes and schools to determine how to best follow these archival policies.

Sexting

Church Personnel should communicate the moral and legal ramifications of "sexting" to the young people they serve as well as their parents. When nude photos of minors are electronically distributed, whether over the Internet or via cell phone transmission, senders and recipients are potentially looking at serious penalties, including jail time and felony charges. Any discussion of sexting should be framed by Catholic teaching about the dignity of all human life.

Social Media

While face to face communication is essential to the social development of young people, online interactions can serve as another platform for communication. As role models for young people, Church Personnel must ensure that the use of social media sites and other online communication is done in a responsible manner. Therefore, social media should never be the primary means of communication with young people.

Church Personnel should take precautions to guard the privacy of anyone who has access to a ministry social media account. The highest privacy settings must be used. In addition, adults should encourage minors who join the online community to set their privacy settings at the highest levels.

Social networking sites, if used, should be one of many resources available to young people or parents. There should always be other ways for information to be shared (Sunday bulletins, parish or school web pages, email campaigns, etc.) Keep in mind that there are young people who do not use social media and still should be included in regular communication.

Appendix B - Signature Page

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 Church Personnel	**Date**

Diocese of Wilmington

Acceptable Use of Technology Church Personnel Volunteer Signature Page

Ministry in a virtual setting must reflect the same principles as those in face-to-face ministry. All technology-oriented activity performed in the execution of ministry to, with, and for young people must be in full compliance with the ethical and moral standards of the Catholic Diocese of Wilmington and its program for safe environments, *For the Sake of God's Children*. This Technology Agreement is an abbreviation of full policies, found in *Technology in Ministry: An Addendum to Ethical Standards for Church Personnel*, 2016. Your signature indicates agreement with full AUP Policy found in www.CDOW.org/FSGC.

- Church personnel are expected to act responsibly and thoughtfully when using technology.
- The use of employer-owned technology and the use of a personally owned technology device on employee-owned grounds or at employer-sponsored events is a privilege not a right.
- Personal use of employer-owned technology is permissible only with permission of a supervisor.
- The employer reserves the right to monitor and track behaviors and interactions that take place online or through the use of technology on employer property or at employer-related events.
- The use of all employer-owned technologies is limited to ministry purposes.
- While the use of personally-owned technology devices (PTD) is allowed at some times, use of these devices must be limited to those times when Church personnel are not actively engaged in the supervision of young people. Such times are rare.
- Church personnel are not permitted to send or take photographs or video with employer-owned technology or PTD on employer property or at parish, school, or diocesan events without advance permission from legitimate authority.
- Devices capable of capturing, transmitting, or storing images or recordings may never be accessed or operated in restrooms, dressing rooms, sleeping areas, or other areas where there is a reasonable expectation of privacy.
- Permission of the parent or guardian must be obtained, in writing, in order for an adult leader to communicate with minors via telephone, cell phone, text messaging, email, social networks, or other electronic means; before sharing/posting pictures or videos of minors; and before sharing email, telephone numbers, or other contact information with other minors or adults who are part of the class, group or organization.
- Church personnel should never consider typed conversations that take place via electronic means (emails, social networking sites, text message, etc.) to be private.
- Church Personnel may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy any individual.
- Church Personnel must be aware of the list of prohibited online activity as defined by the Technology in Ministry: An Addendum to Ethical Standards for Church Personnel.
- Church personnel may not use parish technology to sell, purchase, or barter any products or services for personal gain.

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 Church Personnel	Date