



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

POLICY

It is the policy of the Archdiocese of Miami that digital communications created or transmitted in its name or by its employees or volunteers and/or on technology belonging to the Archdiocese consistently express and support the mission of the Catholic Church to spread the Gospel of Jesus to all people.

I. Mission

Go, therefore, and make disciples of all nations, baptizing them in the name of the Father, and of the Son, and of the Holy Spirit, teaching them to observe all that I have commanded you. And behold, I am with you always, until the end of the age.” (Mt 28:19-20)

The mission of the Catholic Church is to take the Good News of Jesus Christ to all the ends of the earth. The Church preaches this Good News by her words, deeds and actions. Since the Church is the “people of God,” this, too, is the mission of all the faithful, and especially those who are employees of Church institutions.

The Church understands the clear need to use new technologies to spread the Word of God to all people in all generations. The enculturation of the Gospel—especially in language and forms accessible to younger generations—is a complex, but essential task. For evangelization to be effective, it must “use their language, their signs and symbols ... answer the questions they ask, and have an impact on their concrete life” (Evangelii Nuntiandi 63). The National Directory for Catechesis states that “using the media correctly and competently can lead to a genuine enculturation of the Gospel” (NDC 21). “Renewing the Vision: A Framework for Youth Ministry” notes that prosperous ministry with adolescents is, and has always been, built on relationships and effective communication.

The Church is well aware that all the tools for spreading the Gospel are only as effective as those who wield them. This is especially true of 21st century technologies such as the Internet, websites, social media sites and a vast number of “apps.” When used wisely, these tools provide a tremendous impetus to evangelization. When used unwisely, they can damage the mission and ruin lives and careers.

Therefore, the guiding principle in the use of these technological and digital tools is to further the mission of the Church: to spread the Good News of Jesus Christ; to proclaim God’s love; to witness to God’s mercy; and to call others, in Pope Francis’s words, “to discover the beauty of faith, the beauty of encountering Christ.... We need a Church capable of bringing warmth and of stirring hearts.” (Message for 48th World Day of Communications)

II. Purpose



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

- A. In light of the advances in technology, and in view of the fact that much of human communication now takes place digitally — online, via texts, mobile phones, computers and social media — the Archdiocese of Miami compiled this policy regulating the use of digital media and electronic devices by clergy, religious and lay employees, students, volunteers and anyone using technology belonging to the archdiocese.
- B. These guidelines serve to remind anyone using archdiocesan technology that:
 - 1. Everything posted online, searched, sent or received digitally, using equipment — such as computers, servers, smartphones, mobile devices, etc. — and/or services belonging to or paid for by the archdiocese — such as WiFi, email, Office 365, cloud storage / services — is the property of the archdiocese and can be accessed and viewed by the archdiocese.
 - 2. Moreover, everything posted online, searched, sent or received via these services and devices is considered to be public, even if the intent of the employee was to make it private. Anything posted online, searched, sent or received digitally, is by its very nature not private and not erasable or removable.
 - 3. Inappropriate content searched, found on, sent or received via any of those devices can result in disciplinary action against employees, students and volunteers, up to and including termination or expulsion.

III. Definitions

- A. **Blogs:** Online journals that rank posts either chronologically or by popularity. Users can post them on their own website or on blogging sites such as WordPress, Blogger and Tumblr.
- B. **Church personnel:** Anyone — priest, deacon, religious, bishop, lay employee, or volunteer — who provides ministry or service or is employed by an entity associated with the Archdiocese of Miami.
- C. **Content Communities / Online Communities:** That allow users to organize, share and comment on different types of content published by other (not previously known) users.
- D. **Digital Media:** Any technology that allows for the exchange of messages in a digital format.
- E. **Digital Site:** A collection of webpages connected by hyperlinks and belonging to specific locations in the World Wide Web (websites) and other similar digital locations such as clouds, live streaming, FTP sites, and other equivalent services.
- F. **Email:** Any multimedia message (text and/or photos/videos/audio/graphics) that is distributed electronically from one individual to another via a computer network.
- G. **Forums and Discussion Boards:** Internet sites where users can chat, comment, and share documents (ex. Yahoo Chat and equivalents).
- H. **Internet:** A global connection of computer networks.



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

- I. **Microblogs:** Online journals that restrict users to a small number of text/characters per post. Ex: Twitter and Tumblr.
- J. **Mobile Applications:** Most commonly known as Apps; software designed for running in portable devices such as smartphones and tablets.
- K. **Music and Audio Sharing:** Internet sites that allow users to search for music and audio files (ex. Pandora Radio, Spotify and equivalents).
- L. **Podcasts:** Audio files that can easily be transferred over the World Wide Web and embedded in websites.
- M. **Private Social Media Account:** Any social media account created by an individual for personal use only, where the creator of the account does not intend to publish any content on behalf of the entity for which he/she works, whether the content of the account is public or private.
- N. **Public Social Media Account:** Any social media account created by an individual user, whether or not on behalf of an organization, whose purpose is to post content open to the public, so that the wider community has access to the information being shared.
- O. **Rating and Review Sites:** Sites where users can post reviews and ratings of people, businesses, products or services (ex. Yelp and equivalents).
- P. **Social Bookmarking or Social Tagging:** Features that allow users to tag/call out another user's social media account on a specific multi-media content (ex. Stumble Upon and equivalents).
- Q. **Social Media:** Forms of electronic communication (such as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos). (Source / Merriam-Webster Dictionary). These include: Social Networks that allow users to build pages to feature their personal interests or a personal portfolio. Their main purpose is to connect with and share information with friends, colleagues, or previously known contacts. Ex: Facebook, LinkedIn, Snapchat and Instagram.
- R. **Social Media Platform:** Constitutes any one specific social media network site, ex. Facebook, Twitter, Pinterest, Instagram, Periscope etc.
- S. **Text Message:** Any message sent electronically using a digital device. This includes multimedia messages, MMS, IMS, SMS, IRC or equivalent.
- T. **Virtual Social Worlds:** Any computer based software or program that creates a virtual/simulated environment where users can engage in a number of activities (ex. Second Life, World of Warcraft and equivalents).
- U. **Wikis:** Collection of webpages that can be edited by any one internet user to add, change or delete information on a specific topic. Ex. Wikipedia.
- V. **World Wide Web:** A section of the Internet accessed through a user interface containing documents linked together by hyperlinks (Source / Merriam-Webster Dictionary).



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

IV. Digital Communications

This section refers to emails sent or received on any ADOM-owned or ADOM-paid for digital devices or services, including but not limited to WiFi, Internet, computers, smartphones, tablets and other mobile or cellular devices.

A. Data retention

1. Backup of parish / schools information should be performed, at a minimum, nightly.
2. For more detailed information please refer to the ADOM Policy: Record Retention. (We should have a link to this on our e-library but I couldn't find it.)

B. Devices

1. If an ADOM device is not available and/or a personal device is used, any work done on said device on behalf of the ADOM remains property of The Archdiocese of Miami.

C. Digital devices – texting, email

1. All of the above policies also apply to texting. Additional rules apply to educators (catechists/school teachers) or any parish or school staff when communicating with minors.
2. Do not contact minors using a personal email address. Only official Archdiocesan or parish accounts should be used for communication.
3. Copy parents on emails sent to minors. For young children (i.e., elementary school students), only email parents.
4. Do not add young people to personal electronic mailing lists.
5. Have the parents of minors complete Form COM- ? which includes the statement: "I give permission for youth ministry leaders to communicate with my son/daughter using texting, Facebook, email, and other social media. I understand that I may request access to the social media sites, texting and any other electronic communication at any time."
6. If an employee or volunteer receives an inappropriate personal communication from a minor, the employee or volunteer keeps a copy and immediately informs the person's supervisor. Any relevant school or parish protocols are to be followed.

D. Emails

1. Work emails

- a. Every entity — Pastoral Center, parish, school, agency — should have a standardized domain name. i.e. John Smith – jsmith@churchname.org, john.smith@churchname.com, jsmith@bellsouth.net, john.smith@comcast.net, etc. Domain names ideally match the web site address. Entities should refrain from using free email services when possible.



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

- b. All work done on any archdiocesan entity/parish/school system, or using an archdiocesan device and/or service, remains the property of said archdiocesan entity/parish/school/system.
7. Non-work emails
 - a. Any archdiocesan work done on personal email systems and/or free email systems remains the property of the Archdiocese of Miami.
 - b. Electronic retention policy should be followed at all times by all entities (Please see point 5 for more information).
8. Electronic voicemail
 - a. When the technology is available and a voicemail gets transferred to the employee's email, it should be treated as an email.
 - b. All rules applying to emails apply to electronic voicemails.
9. Network
 - a. Any work done on any archdiocesan system, school system, parish system, archdiocesan device and/or service remains the property of said archdiocesan / school.
 - b. When using an Archdiocesan system and/or device "best practices" should be followed with respect to content.
10. Proprietary Digital Information
 - a. Proprietary information (contact information, documents, graphics, e-mail, etc) stored on the electronic device must remain and may not be deleted, modified, copied or otherwise removed from the parish/school/entity network.
 - b. Record retention section of the policy must be consulted.
11. Recording Devices
 - a. When using tape/digital/telephone to record conversations, the consent of the person being recorded must be obtained beforehand, in order to comply with Florida laws, which forbid recording of conversations without the consent of all parties.

Social Media

Church personnel should be aware that they represent the Church and the archdiocese by nature of their employment and/or ministry. Therefore, they should exercise prudence and discretion in posting on any social media sites, be they public or private, personal or professional. They need to be aware that online activity indicative of prohibitive behaviors may subject an employee to disciplinary action or termination, and a volunteer to a discontinuation of service. Church personnel working in positions of leadership may be held to a higher standard in this regard.



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

A. Set-Up and Management of Social Media Accounts

12. Branding:

- a. For purposes of branding and clarity, social media pages should be limited to one per parish and one per school per social media platform — i.e., one on Instagram, one on Twitter, one on Facebook. However, if more than one account is necessary (i.e. a school alumni or sports page, or a parish group page), each one should follow the approval procedure stipulated below by the Archdiocese of Miami.
- b. Each parish/school/group/entity's social media sites should be clearly identified as belonging to the parish with the parish's name and logo and a link to the official parish website (when applicable). Each site should also clearly identify itself and its purpose in the description or "about me" section of the social media platform.
- c. Each authorized page also must be verified as “official” by the appropriate social media platform.
- d. It is recommended that the parish's social media account "follows" the official account of the Archdiocese of Miami (when applicable) to make its association with the archdiocese clear.
- e. Where appropriate, age restrictions should be enforced.

13. Authorization

- a. Those wishing to open a social media account/page on behalf of any Archdiocese of Miami entity, such as a parish, school, ministry, or group, should receive permission from the appropriate supervisor, whether this be the pastor, principal, or department director, prior to opening the account.
- b. The appropriate supervisor should appoint account administrators, that is, those who will have access to the account and permission to post on the page as well as monitor and delete comments. The names and contact information of these administrators should be kept by the same supervisor, should there be the need to request the deletion of any piece of information.
- c. Each account should have a minimum of two and a maximum of four administrators, including the supervisor, who will share the responsibility of monitoring content that is published in the account. The supervisor does not need to exercise regular administration of the social media account, but he/she must have access to log-in information and passwords, and the ability to delete comments, remove posts, add and remove other administrators as well as deactivate the social media account, if necessary.
- d. Once approved, the administrator of the page should notify the Department of Communications of the Archdiocese of Miami, as well as any other related archdiocesan department or ministry (such as the Department of Schools in the case of a school social media account), regarding the creation of the account/page. The administrator must provide the Communications Department and the



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

appropriate department or ministry with the account(s) login and password information, should the department or ministry need to log-in in case of a social media emergency.

- e. Only approved managers/administrators are to post on social media accounts belonging to the Archdiocese of Miami or one of its entities. Login information should be known only to these individuals and the appropriate supervisors.
- f. The name of the parish, school or ministry cannot be part of any social media page or group without the appropriate supervisor's approval.

14. Content

- a. Content posted to any ADOM social media account should be reflective of the values and teachings of the Catholic Church and should have the ultimate purpose of evangelization.
- b. The Archdiocese of Miami and its entities hold the intellectual right to all its original content posted on its social media sites. When third party content is shared, the source of the information should be well-noted, to clearly state that it is not coming from the Archdiocese of Miami.
- c. All archdiocesan employees and page administrators must comply fully with copyright law when posting on social media. (See copyright section ?)

15. Comments

- a. Social media accounts should be monitored on an ongoing basis. Digital notifications should be set up for all administrators of the social media account, so it is easier to manage comments and keep track of what activity is happening with the account. In most cases, digital notifications can be set up under the settings tab of the social media platform.
- b. Some social media platforms such as Facebook allow for the manager to set up profanity filters, so that comments with specific words are blocked. It is a best practice to set up profanity filters for an account whenever possible.
- c. Comments should be accurate and charitable in tone and should augment the conversation. Users are free to express their opinions concerning the different topics posted in the account as long as they do so in a respectful manner without insulting and/or disrespecting others.
- d. Comments that violate the rules and regulations explicitly expressed in the "about" section of the page or profile can be eliminated (upon the discretion of the page's administrator).
- e. Dissenting comments, but that are expressed in appropriate language and without insulting other users should be allowed to remain in the page.
- f. Comments should not include foul language or language that would damage the reputation of an individual, that are libelous, or that are insulting in nature.



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

- g. Inappropriate comments should be deleted as soon as possible and, if necessary, the user who posted the comment should be blocked at the same time.
 - h. If the social media platform allows for sending notifications or alerts via email to the administrator/s regarding comments that are posted, the administrator(s) should choose that option.
 - i. "Guideline on Appropriate Conduct" section should be included (when possible) in the biographical/about area of the platform detailing to users what constitutes appropriate and inappropriate comments and conduct, and the actions that will be taken should a conduct or comment be deemed inappropriate.
 - j. Questions formulated by the user should be answered by the administrator on a timely basis.
 - k. The administrator should seek the approval of the supervisor before answering sensitive questions posed by users.
 - l. If any questions arise on how to answer a user, contact the Department of Communications of the Archdiocese of Miami for assistance.
16. Blocking of users
- a. When a user violates the rules and regulations of the page as set by the administrator(s).
 - b. When there is verbal abuse against another user or against anyone. Verbal abuse includes use of profanity, language that is unkind or that is said with the intention of bullying another user.
 - c. When a user uses language that is libelous.
 - d. When a user has a consistent pattern of spamming/trolling.
17. Personal social media accounts (pertains to ADOM employees)
- a. Employees of the Archdiocese of Miami are expected to keep their personal social media accounts separate from the archdiocesan accounts.
 - b. Employees should refrain from making use of their personal social media accounts during working hours.
 - c. Employees cannot disclose insider, proprietary or confidential information about the Archdiocese of Miami on their personal social media accounts. If they do, they may be legally liable.
 - d. Employees cannot use, on their personal social media sites, the Archdiocese of Miami crest/logo for purposes of self-promotion and/or to promote a product, candidate, a political party or a cause. If they do, they may be legally liable.
 - e. Employees should remember that nothing is private once it is posted on the web, and all posts are searchable through search engines. In other words: The Internet never forgets. Don't do anything online you would not do in public.



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

- f. If the employee self-identifies as an Archdiocese of Miami employee on a social media site or posts comments identifying himself/herself as an archdiocesan employee, he/she should make clear that the views are his/her own and the employee is not posting them as a representative of the archdiocese. Employees are advised to include a disclaimer in their "about me" section with a sentence similar to this: "The views expressed on this [social media site, blog etc.] are mine alone and do not necessarily reflect the views of the Archdiocese of Miami."

V. Minors

The Catholic Church is committed to keeping children and youth safe. When using any form of social media, all Church personnel will abide by the requirements of civil law and follow the "Recommended Technology Guidelines for Pastoral Work with Young People" that have been developed and published by the National Federation for Catholic Youth Ministry in Consultation with the U. S. Conference of Catholic Bishops. This applies to all Church personnel, including, but not limited to: employees in schools, volunteers in schools, and those running afterschool programs (whether employees, volunteers or contracted vendors) such as sports, drama, any extra-curricular programs, employees in the parish, directors of religious education, youth group ministers, volunteers in the parish such as catechists and youth group leaders, any ministry leader or volunteer.

Specifically, Church personnel must comply with all aspects of the Children's Online Privacy Protection Act (COPPA), which forbids the posting or distribution of personally identifiable information of any child (under the age of 13) or minor (under the age of 18) without parental consent. Personally identifiable information includes name, home address, email address, telephone number or any information that would allow someone to identify or contact a minor.

A. Consent forms

1. If written verifiable consent is obtained from a parent, it is important that the parent have approved the information and have full knowledge of its use, purpose and how it is to be provided.
2. Upon request, parents need to have access to anything provided to their minor children. For example, parents need to be made aware of how social media is being used, how to access the site(s), and be given the opportunity to be copied on all material sent to their minor children via social networking (including text messages). While parents should be provided with the same material as their minor children, this does not have to be done via the same technology (that is, if minor children receive a reminder via Twitter, parents can receive it in printed form, or via email.)
3. In order to inform parents of their rights and responsibilities, the following notification will be included in permission forms for children and minors: "I give permission for youth ministry leaders to communicate with my son/daughter using texting, Facebook, email, and other social media. I understand that I may request access to the social media sites, texting and any other electronic communication at



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

any time."

4. Media consent forms should be distributed at the beginning of the school or catechetical year, at the first youth ministry meeting, or whenever a new student or group member joins. These consent forms must be signed by the minor's parent or guardian and returned to the school, catechist or youth minister. Consent forms should specifically mention social media (see above). Sample consent forms (Form #) are available from the ADOM Communications Office and in the e-library.

B. Photographs and video

1. Photographs or videos depicting minors should be cleared beforehand by consent forms.
2. Should a post include an image of a minor whose consent form was not returned or not signed, that post should not be published on social media. If already published, it should be taken off immediately, and the school's procedures should be followed.
3. Should there be doubts about whether or not to post a piece of content, the manager/administrator of the account should contact the appropriate supervisor and/or the Communications Department of the Archdiocese of Miami for guidance.

C. Social media and schools

1. Teachers seeking to create social media accounts for class purposes should get the approval of the appropriate supervisor (principal) and should have a minimum of three adult administrators. The teacher should inform the students' parents regarding the creation of the social media account and give them access to the account in order to monitor the content that is published.
2. Content should be strictly restricted to school-related activities.
3. No contact should be made directly to a student through the social media account, including texts or direct messages.
4. All posts by the teacher should be made in general to the whole class.
5. Teachers should only respond to students' legitimate school-related questions, and then only via the comments section on the social media site.

D. Social media and religious education programs

1. Catechists should abstain from creating social media accounts to communicate with their students, even if for class purposes.
2. Should there be a need to create a social media account for class purposes, the Catechetical Leader should seek the approval of the appropriate supervisor (pastor) and follow the same rules outlined in this document for parish's social media accounts.
3. In addition, parents of all religious education students who are minors should have access to the social media account.
4. Only images of children/ minors engaged in public school/parish/catechetical



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

activities may be posted on social media, after having obtained previous permission from their parents. This could be done via a form attached to a school handbook or catechetical registration, which would be signed by the parent and retained in the school/catechetical records.

5. Under no circumstances, should inappropriate images of minors be posted or displayed in the social media account.

E. Communication with minors

1. No Church personnel should have one-on-one contact with minors via phone.
2. In an emergency situation, a phone call may take place if on speaker phone with a supervisor present.
3. All telephone communication should take place with the parent or guardian of the minor.
4. All text messages should also include, simultaneously, the parent or guardian and a supervisor.

VI. Voicemail

A. Transferring Phone Calls:

1. As a standard rule, to transfer a call correctly you must ask the caller to hold, call the extension to which he / she wishes to be transferred to, then mention that you will be transferring a call and the reason why the caller is on the line. Then go back to the caller, give them the extension number in case they get disconnected and tell them you will now transfer them to that extension.

B. Voicemail greetings:

1. Voicemail greetings should be consistent throughout archdiocesan entities and should include the following elements:
 - a. First and last name of the person usually available at the phone extension;
 - b. Name of the organization followed by the name of the Department
 - c. Request for the caller to leave his/her contact information and a brief message

C. Parish bulletins

1. All parish bulletin editors must be approved by the pastor to write/design/produce the bulletin for the parish.
2. Editors must seek final approval from the Pastor for all content to be published in the parish bulletin before the bulletin is sent to print.
3. On occasion, the Parish Bulletin Editor will receive information from Archdiocesan offices such as the Chancellors' Office or the Communications Department, or in the Pastoral Bulletin, for inclusion in the parish bulletin. It is important for the editor to include the information as requested.



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

4. Should the parish bulletin editor receive information from any other department of the Archdiocese of Miami, it is the editor's responsibility to seek clearance first from the Chancellors' Office.
5. If a Parish's designated parish bulletin editor changes, it is the responsibility of the new editor to contact the Chancellors' Office and the Archdiocesan Communications Department to inform them of the change and provide the new contact information (if applicable).

VII. Security

Access to ADOM /parish/schools systems should only be provided to authorized personnel; this includes but is not limited to wired/wireless connections, emails, devices, passwords and log-in information, etc.

VIII. Responding to Emergencies

- A. Any comment that raises a concern related to security or safety should not be deleted until reported to law enforcement and law enforcement has advised that the comment may be deleted. If in doubt, contact the Communications Office before deleting.
- B. Upon learning of a social media emergency, the Office of Communications of the Archdiocese of Miami should be contacted and the Director of Communications informed concerning the issue.
- C. If the issue is of a serious nature (ex. involving inappropriate images) contact the proper law enforcement authorities in addition to informing the Office of Communications of the Archdiocese of Miami.

IX. Legal matters

- A. Anti-bullying
 1. Bullying may involve but is not limited to: teasing, name-calling, slurs, rumors, jokes, false accusations, intimidation, stalking, innuendos, demeaning comments, pranks, social isolation, gestures, cyber-bullying or other verbal or written conduct. Cyber-bullying includes the following misuses of digital technology: teasing, intimidating, or making false accusations about another student by way of any technological tool, such as sending or posting inappropriate email messages, instant messages, text messages, digital images or website postings (including blogs and social network sites).
 2. The Archdiocese of Miami is committed to promoting a safe, healthy, caring, and respectful environment for all of its employees and the people it serves. As such, bullying is strictly prohibited and will not be tolerated. Therefore, this policy prohibits any unwelcome verbal, written or electronic conduct or gestures directed at any individual that has the effect of:



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

- a. Physically, emotionally, or mentally harming the individual;
 - b. Damaging, extorting or taking an individual's personal property;
 - c. Placing an individual in reasonable fear of emotional or mental harm;
 - d. Placing an individual in reasonable fear of damage to or loss of personal property;
or
 - e. Creating an intimidating or hostile environment.
- B. Reporting complaints
1. Every affected individual has a duty to report any bullying to the appropriate entity immediately.
 2. False reports or accusations of bullying also constitutes a violation of this policy and may subject the offending party to appropriate disciplinary action.
- C. Retention of electronic records
1. The term "electronic record" means any record that is created, received, maintained or stored in Archdiocesan work stations or central servers. Examples include, but are not limited to: email, Web files, text files, PDF documents, word processing documents, spreadsheets, databases, database data, backup tapes, and other formatted files.
 2. The legal custodian of an email message or an electronic document is the Archdiocesan employee that originates the messages or to whom the email message or electronic document is sent. If the record is transferred, by agreement or policy, to another person for archival purposes, then that person becomes the legal custodian.
 3. It is the policy of the Archdiocese that electronic records must be managed in the same way as traditional records to ensure compliance with state and federal regulations and to preserve institutional history. In the event of litigation or notice that litigation is imminent, Litigation Hold policies will apply to electronic documents as well as paper documents.
- D. Electronic mail
1. Not all email needs to be retained, depending on the subject matter. Work related email is an Archdiocesan record, and must be treated as such. Each email user must take responsibility for sorting messages and retain Archdiocesan records as directed in the Archdiocese of Miami Policy: Record Retention.
 2. Email that does not meet the definition of a record of the Archdiocese, such as personal or junk email, should be deleted immediately from the system.
 3. Email servers are not intended for long-term record retention periods and are to be printed and filed in similar fashion to paper records. It is important to note that the email message should be kept with the attachments.
 4. Archdiocesan offices only will archive email for up to 12 months after which time the email will be permanently deleted. (For other specific email policies, refer to the



ARCHDIOCESE OF MIAMI DIGITAL COMMUNICATIONS POLICY

Digital communications section above.

E. Ownership

Any technological tools that are used by employees or volunteers in the Archdiocese of Miami, such as websites, blogs, social network sites, and the like, are the property of the Archdiocese of Miami.

F. Copyright laws

All Church personnel must comply fully with copyright law including when using social media and technology. The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Archdiocesan entity.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Archdiocesan entity or the end user does not have an active license is strictly prohibited. Public disclosure of information about programs (e.g. source code) without the owner's authorization is prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

G. Penalties / Enforcement

1. It is the responsibility of every authorized person to know these guidelines and to adhere to them. Users who disregard these policies may be subject to a disciplinary action up to and including termination or removal from their volunteer position. Anyone with knowledge of an individual who is inappropriately using or has disregarded the digital communications policies mentioned in this document is also in violation of these should he/she not report it verbally and in writing to the individual's supervisor.
2. Failure to abide by this policy may result in disciplinary or legal action by the Archdiocese of Miami.
3. Finally, it is the responsibility of each entity (parish, school, other entity) to monitor the social media sites created by staff and ministry leaders.

Initial: November, 2017

Current: November, 2017