Social Communications Policy

Updated February 2018

Social Communications

Social Communications deals with the all the problems raised by the cinema, radio, television, the daily and periodical press, and digital media in relation to the interests of the Catholic religion.

Standards for All Social Communications Policies

1.0 Glossary of Terms

1.1 Authorized User - Any church personnel who has been authorized by a senior level manager of the entity of which he/she represents to use diocesan owned technology as it pertains to that specific entity.

1.2 "Administrator": A person who is authorized to have full control over an approved technology. Approved technology includes but is not limited to, computer networks, email systems, domains, social media sites or other cloud based solutions. An administrator must have written permission of pastor or immediate supervisor.

1.3 "Church Personnel": For purposes of this policy only, Church Personnel includes all individuals who minister, work, or volunteer in any school, parish, or ministry of the Diocese whose compliance with this policy is sought. The term has no legal meaning or significance outside the scope of this policy and is not indicative of any employment or agency relationship.

1.4 "Consultant": Independent contractors, consultants, vendors or other persons who are not subject to the supervision of the Bishop of the Diocese and for whom no such duty to withhold payroll taxes exists, but provide expertise on database creation and/or management, IT services, or internet-related services.

1.5 Diocesan entity: Any parish, school, entity or ministry of the Diocese of Orlando, including those entities which are separately incorporated under 501 (c) (3).

1.6 Domain: The unique internet registered address of the entity. The Domain should be registered in the name of the entity and used for all official business and email.

1.7 "Employee": Any lay person who is employed by any Diocesan entity, whether part-time or full-time, who is given payment for services rendered, and for whom the Diocesan entity is obligated to withhold payroll taxes (FICA, Medicare, and withholding).

1.8 Group Social Media Site: This site is also known as a list serve or discussion forum. A group site can only be viewed by invitation or request. The administrator knows the people who are members and the members can interact. In Facebook, groups can be open, closed, or secret. The members and content of an open group are public. In a closed group, the list of members is public, but the content is private. In a secret group, the members and content are private, and the group doesn't appear in search results for non-members.

1.9 Internet: Includes both external and internal access of communications and data storage equipment, either owned or reserved for use by the Diocese, by digital information devices including personal computers (PCs), personal digital assistants (PDAs) and similar devices. The term "Internet," as it applies to external resources, is meant to be all-inclusive and comprises other similar or analogous terms such as the "world wide web," "e-mail," and "the Net."

1.10 Internet/Intranet/Extranet-related systems: include, but are not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing and FTP.

All internet/intranet/extranet-related systems are the property of the Diocesan entity it serves. These systems are to be used for business purposes in serving the interests of the Diocesan entity, its staff, and its constituents in the course of its normal operations.

1.11 IT: Information Technology

1.12 Network: Communications system connecting two or more computers and their peripheral devices to exchange information and share resources.

1.13 Personal Social Media Site: Personal social media sites are created by an individual to stay connected with family and friends, and to interact with the online community—not for the purpose of ministry.

1.14 Public Social Media Site: A site that an administrator creates for public viewing. It is open to anyone who has internet access and therefore the administrator does not know the identity of the people who view or interact with the site.

1.15 Social Media Site: Any online technology that allows individuals to interact on some level to share information, dialogue or stay digitally connected. This includes many well known sites for video sharing such as YouTube, social networking such as Facebook and microblogging such as Twitter. This policy does not list the approved social media sites because it is only intended to provide guidelines which should be applied to the digital media landscape which is ever changing. Social media includes web-based and mobile based technologies which are used to turn communication into interactive dialogue among organizations, communities, and individuals. Andreas Kaplan and Michael Haenlein define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."[1] Social media is ubiquitously accessible, and enabled by scalable communication techniques.

1.16 Spam: Unauthorized and/or unsolicited electronic mass mailings.

1.17 "Volunteer": Any unpaid person engaged or involved in a Diocesan activity, specifically as it relates to database creation and/or management, IT services, social media, or internet-related services.

1.18 Contributor: Any paid or unpaid person who provides content (photo, text, video) for a social media post. A contributor may be assigned the "editor" role on Facebook to post content, as long as the content is regularly approved by administrator.

2.0 Scope

These policies apply to authorized users of any school, parish, or ministry of the Diocese of Orlando, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Diocesan entity.

3.0 General Standards

3.1 Links

All Diocesan parishes, schools, and entities must have a link for the Diocese of Orlando website, www.orlandodiocese.org, and may have links to other Diocesan entities, such as San Pedro Center, www.sanpedrocenter.org; Catholic Charities of Central Florida,

[1] Kaplan, Andreas M.; Michael Haenlein (2010) "Users of the world, unite! The challenges and opportunities of Social Media". Business Horizons 53(1): 59–68.

www.cflcc.org; and Bishop Grady Villas, www.bishopgradyvillas.org on its own website. Any other links should not be in conflict with the teaching and the Magisterium of the Roman Catholic Church. Acceptable links fall into these three main areas:

1. Official Church sites, such as the Vatican, U.S. Conference of Catholic Bishops, state conferences, archdioceses and dioceses;

2. Parts of the Diocese such as parishes, schools and ministries operated by the Diocese or approved resources associates with those ministries; and

3. Those under the oversight of a bishop or religious congregation, or listed in the Official Catholic Directory. Church leaders should use prudence in evaluating links to other commercial opportunities on its site. It is the entity's responsibility to evaluate its hosts' advertisers and sponsors on a regular basis.

3.2 Photos

Photos may be posted or published on a social media site or website. Tagging or identifying the person(s) in the photo is not allowed unless an individual gives permission to be identified.

1. Use of photos on websites should be group photos. Where children are involved, no names or first names only should be used. Parents/guardians must sign permission slips each year for use of children's photos; therefore, all photos, particularly those which include children, should be refreshed regularly.
2. Recording/Photography by Family/Friends: A parish/school/entity of the Diocese cannot be held responsible for recorded materials (e.g. audio, still and/or video) transmitted or placed without its knowledge or permission through electronic or other means or in external media of any type. For its official, sanctioned electronic resources, a parish/school/entity of the Diocese of Orlando has established acceptable use standards for recorded materials. It is suggested that parents and guardians follow these standards in their personal activities and on their Personal Social Media Sites. As such, parents, guardians, family members and friends who photograph or otherwise record school/parish/entity events should respect the privacy of others and should not identify another child by more than a first name in any transmission (e.g. mail, e-mail or internet website), unless authorized by the parent or guardian of that child.
3. Parents/guardians must sign permission slips each year for the use of video where children are present. Use of videos on websites should be refreshed regularly when images of children are present.

3.3 Catholic Identity

Information posted using any form of technology in the name of the Church must adhere to the following guidelines:

a. Content or information should be appropriate and affirm the teachings of the

Catholic Church and its Magisterium.

b. Must be professional, respectful and courteous.
c. Must avoid debate of Catholic Church teaching.
d. Have the pastor (or supervisor) monitor content on a regular basis.
e. Only logos or photographs of ministries/organizations/vendors directly tied to the Catholic Church /or an approved site may be displayed on the page.
f. There shall be no offensive or disruptive messages, initiated either by the administrator or user. Among those which are considered offensive include, but are not limited to, messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment which offensively addresses someone's age, sexual orientation, belief system, national origin, or disability.

3.4 Transparency

1. It is essential to the nature of ministry that parents/guardians are fully aware of all mediums being used to keep in contact with their young person for ministerial purposes.

2. The intent of any communication policy is to give witness to the Good News to create a safe environment for all vulnerable populations, which is open, transparent and involves the parents/guardians of the young people as partners.

3. It is important that ministry is not used to establish private one-on-one relationships between adults and youth and our methods of communication must reflect this.
   - Adults must maintain copies of communication with youth (under 18) and copy parents on all e-mails and other electronic correspondence.
   - Adults must copy supervisor on individual correspondence with young adults (over 18) who have not completed high school.
   - Adults should copy supervisor on individual correspondence with young adults who have completed high school.

4. Unusual circumstances of a pastoral nature should be documented and shared with the pastor or one's supervisor as soon as feasible. The documentation of any such circumstance should involve a copy of any applicable communication from all types of communication medium.

5. The administrator's log on credentials must be shared with the pastor or appropriate supervisor. In addition, the administrator must provide credentials on any account on which the administrator has privileges. Administrator passwords may not be shared with others.

6. Leaders of ministry must say "no" if asked to be a friend on a social media page of a youth (under 18) and should say "no" to parents, parishioners or other individuals who interact with them only through this leadership role. There are risks with social communications, especially with blurring boundaries of professional and personal relationships. Anyone can say "no" to someone who wants to be their friend. Ultimately, what employees do on their own time is governed by the Diocesan conduct policy.

4. Enforcement

Effective security is a team effort involving the participation and support of every authorized user who is using social communications. It is the responsibility of every authorized user to know these guidelines, and to conduct their activities accordingly. The Diocese of Orlando does not sanction any use of social communications that is not authorized by or conducted strictly in compliance with this policy and its regulations. Authorized users who disregard these policies may be subject to a change in their relationship with the Diocese, up to and including termination or removal from their volunteer position. In addition, any Employee found to have violated this policy may be subject to disciplinary action, up to and including termination. Administrators who have read and signed the Agreement and who agree to act in a considerate and responsible manner will be authorized users.

These rules are in place to protect authorized users and Diocesan entities. Inappropriate use exposes Diocesan entities to risks and legal issues. Anyone with knowledge of inappropriate use of social communications that is in violation of this or any other Diocesan policy should report this information verbally and in writing to the individual's supervisor.

4.1 Disciplinary or Legal Action

Failure to abide by this policy may result in disciplinary or legal action by the Diocese of Orlando. It is the responsibility of each entity (parish, school, other entity) to monitor the social media sites created by staff and ministry leaders.

Social Media Policy

1.0 Overview

Why Are Catholics Called to Use Social Media?

Social media is a fast growing form of communication in the United States among people of all ages. Our Church cannot ignore it, but instead engage social media in a manner that is safe, responsible and pastoral.

"…the new communications technologies must be placed at the service of the integral good of the individual and of the whole of humanity. If used wisely, they can contribute to the satisfaction of the desire for meaning, truth and unity which remain the most profound

aspirations of each human being." Pope Benedict XVI, World Communications Day Message, June 5, 2011

Pope Benedict XVI also sends this note of caution: "Who is my "neighbour" in this new world? Does the danger exist that we may be less present to those whom we encounter in our everyday life? Is there is a risk of being more distracted because our attention is fragmented and absorbed in a world "other" than the one in which we live? Do we have time to reflect critically on our choices and to foster human relationships which are truly deep and lasting? It is important always to remember that virtual contact cannot and must not take the place of direct human contact with people at every level of our lives."

Social Media is to be utilized as a particular tool to continue the work of ministry, the purpose of which is to invite those whom we serve to become living disciples of Jesus Christ. It is essential that our ministries utilize the tools to that end, rather than being shaped by the technology itself.

Social media can only be one part of a multi-faceted approach to reach out to others and invite them to a life in Christ, in community, for the greater good of society. Information shared via a social network should also be available on a traditional website, one on one, in groups and via multiple channels of communication. This includes everything from personal conversations and phone calls, to the bulletin, flyers and mailings. The focus is evangelization, social media is simply one more tool, and not the end in itself.

- Social media is the online technology and methods that allow people to share content, personal opinions and insight with others. It implies a two-way communication between parties. It is not static. Content can come in many forms: text, images and photos, video, audio. It allows people to create a personal profile about yourself and then share and discuss with your circle of accepted friends and family. Example: Facebook
- Social bookmarks allow you to publicly share your list of favorite websites. Example: Delicious Online gaming allows users to interact with others for the purpose of an online game. Example: AdventureQuest
- Blogging allows people to write and publish their thoughts and opinions and have others provide instant feedback. Example: Wordpress
- Microblogging allows you to post in a short amount of characters information about your daily schedule or micro current event as it happens. Example: Twitter

Digital media is a form of electronic media where data are stored in digital (as opposed to analog) form. It can refer to the technical aspect of storage and transmission (e.g. hard disk drives or computer networking) of information or to the "end product", such as digital video, augmented reality, digital signage, or digital art. Florida's digital media industry association, Digital Media Alliance Florida, defines digital media as "the creative convergence

of digital arts, science, technology and business for human expression, communication, social interaction and education". Digital Media does not imply two-way communication between parties.

- Wikis allow you to create, edit and share information about a topic. Example: Wikipedia
- Video sharing allows you to upload and share video with others. Example: YouTube.
- Photo sharing allows you to upload photo and images that can be viewed by others. Example: Flickr and Pintrest
- News aggregator, also known as a feed aggregator, feed reader, news reader, RSS reader or simply aggregator, is software or a Web application which aggregates syndicated web content such as news headlines, blogs and podcasts in one location for easy viewing. Example Digg

2.0 Social Media Sites

2.1 Approval Process

You must request permission from your pastor, principal or appropriate supervisor about the formation of a social media site prior to its creation. If approval is granted, the administrator must sign a "Social Media Administrator Agreement" and the agreement should be filed with the appropriate supervisor.

2.2 Choosing an Administrator

In order to ensure content on a social media site is accurate and true to the Magisterium of the Catholic Church, it is important to have a administrator that understands Catholic teachings and can communicate them effectively. The administrator must have written permission of pastor or immediate supervisor and be a diocesan employee who is a senior manager of the organization. This will allow the responsibility of ensuring proper content is posted and proper polices are followed to be managed by the diocesan employee. The administrator log on credentials should be shared with the pastor or appropriate supervisor.

2.3 Administrative User Names and Passwords

Administrative account contacts for websites, email systems, discussion groups, social media accounts or any other service whether hosted internally or externally should be a senior manager of the organization who has responsibility over the Information Technology function. User name and password information for management of these services must be maintained by each entity in a safe and secure location. The location should be known only to the appropriate IT authority and a senior manager such as Pastor, Principal, Business Manager or CFO.

2.4 Professional Account for Ministry

Social media site accounts should be formed independently of a person's *Personal* Social Media account and personal email address. The email address used for the establishment of the account must correspond with an entity email domain.

2.5 Comments

When possible, select the option to moderate comments before they are posted. There should be a comment policy on the social media site that explains what is allowed in terms of commenting. The public may comment on the administrator's posting as long as they follow the comment policy. An administrator should block anyone who violates the comment policy or displays any inappropriate conduct.
If there is an option to have comments or notification or alerts sent to your email, choose this so you will be aware of comments in a timely manner.

Comment monitoring means that you check your social media site on a regular basis and if someone has left a comment, you formulate a response and reply. If there is an inappropriate comment, you remove it and then you block the user (per your comment policy).

The Diocese of Orlando follows the comment policy of the United States Conference of Catholic Bishops.

The purpose of any a social media page is to provide an interactive forum where readers can gather and discuss information about the wide range of issues addressed by the work and mission of the Catholic Church, specifically through the Diocese of Orlando.

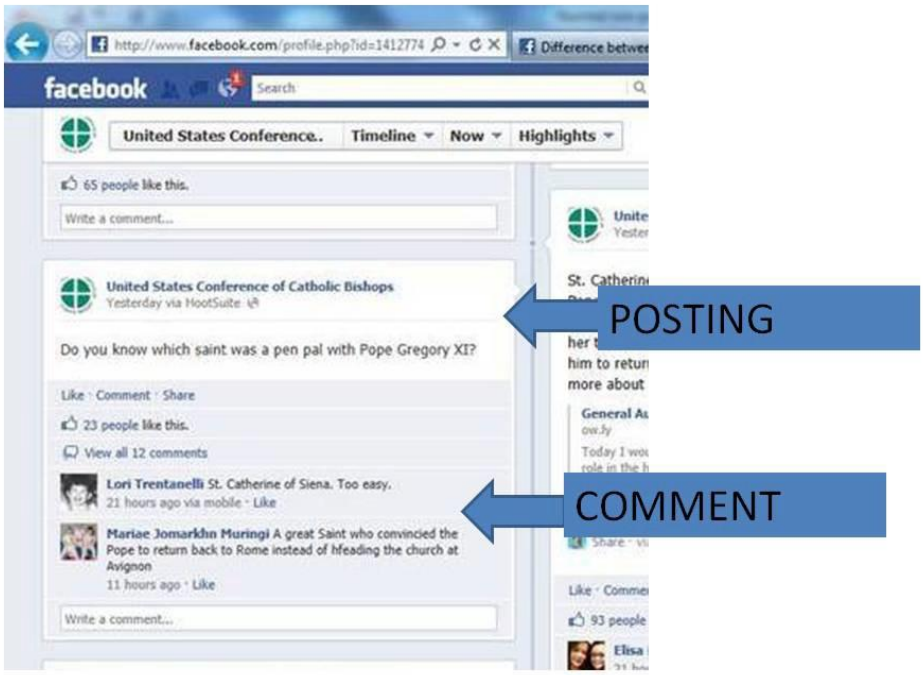
Followers are encouraged to post questions, comments and concerns, but should remember this is a moderated online discussion hosted by the Diocese of Orlando.

The Diocese of Orlando appreciates healthy, constructive debate and discussion; that means we ask that comments be kept civil in tone and reflect the charity and respect that marks Christian discourse. Comments that may be deleted include those that contain:

- Personal attacks/inflammatory remarks against a person or group
- Content/comments off topic
- Spam
- Links to sites that contain offensive material or attack the Church's hierarchy and its mission
- Promotion of services, products, political organizations/agendas
- Information that is factually incorrect
- Vulgar Language

The Diocese of Orlando reserves the right to remove posters who violate this policy. All sites must state that "Comments left by others on this page do not reflect the views of the Diocese of Orlando."

2.5.1 The Difference Between a Posting and a Comment:



2.6 Fan/Follower/Member Photos

If the option exists to hide the fans, followers, etc. choose this. Otherwise, monitor the profile photos of your fans, followers, etc to remove anything that appears inappropriate.

2.7 Posting

Because our faith is alive and the content of your social media site should be ever changing, it is advised that you visit your site regularly for updates and to address any concerns within 24 hours or sooner if possible.

2.8 Social Media Associations

Some public social media sites allow you to follow others as a form of social engagement. Official diocesan/parish/school/entity social media sites used for ministry should not follow individuals such as parishioners, clients, minors. Also, they should not link to other online sites that support or oppose candidates or political parties. Consult with your diocesan attorney or the Florida

Conference of Catholic Bishops before posting any political content or links to political content on web or social media sites.

Official diocesan/parish/school/entity social media sites are requested to follow diocesan social media accounts such as https://twitter.com/orlandodiocese, https://twitter.com/BishopNoonan and https://www.instagram.com/orlandodiocese. It is also acceptable to follow entities as described in General Standards 3.0 and Links 3.1 of this policy, (page 5).

3.0 Instant Messaging

No instant messaging between youth and Ministry Leaders through a personal computer or other electronic device is permitted.

4.0 Age Restrictions

If there is an option to restrict access to a public social media site by age, the age limit should be defined as 13 and over. Minors under the age of 18 cannot join Facebook groups or other type of interactive opportunities unless total transparency and privacy is ensured. For those who are 18 years and younger (high school or elementary school students), Facebook "secret" groups are not allowed.

5.0 Advertising

Select to remove advertising when possible. Monitor the advertising and report anything inappropriate. Include a disclaimer on your social media site that you are not responsible for the content of the advertising and it is beyond your control.

6.0 Website Updating

A best practice is that information about an entity's events, activities and ministry appearing on a social media site is also reflected on the entity website so that the information is accessible in both areas. It is the administrator's responsibility to provide the content to the website manager at the same time that the information is posted to the social media site.

Unless serving in a dual role, the administrator is not responsible for how and when the website information is updated. If the administrator of the social media site is the website manager, this process can be more effective. If the website has an application that allows for simultaneous updating of social media sites and website, the process will be more effective.

7.0 Multiple Social Media Outlets for an Entity

There can be more than one social media site for each entity, if there is good reasoning for the use of multiple sites. No one should create a social media site in a vacuum. Pastors,

principals, supervisors should be engaged in the conversation to determine its appropriateness and process. Planning ahead to determine the total need and coordination of branding and information sharing in real time is important in order for the sites to maintain their integrity and use. A qualified administrator who understands the nature of social media sites and the symbiotic relationship between them is important in planning for these sites.

8.0 Public Social Media Sites

Example of Public Social Media Sites include: "Facebook Page" and Twitter account.
It is appropriate to use a public social media site for general information about happenings, current events and liturgical information, saints of the day, surveys, etc. For example, post information you would want to appear on the front page of a local newspaper or on the broadcast news.

When setting up a public site, it is best to limit the level of participation of the members who join this community, Any social media site that is designed for public viewing should be set up so that only the administrators or approved contributor is allowed to post status updates, photos, videos or other content

9.0 Group Social Media Sites

Sharing of ministry best practices, upcoming events, rules and regulations as well as the opportunity to provide input can occur through group social media sites such as discussion groups, forums, list serve groups and others. Members of this community may comment as long as they follow the comment policy.

9.1 Permission Levels

The administrator of a group social media site may decide the permission level they would like to give to their members. A policy regarding permission levels should be recorded and followed by the administrator, in collaboration with his/her superior(s). The application used for these purposes must offer a tracking system.

9.2 Persons Selected for Group Participation

1. Must be within the same field or position of the administrator of the group.
2. Must request to participate and be approved by administrator, or be invited to participate by the site administrator.
3. Pastor and immediate supervisor should have ability to access group, and requirement of a minimum of 2 administrators should be maintained.

9.3 Monitoring of Group Speak

1. Administrators should monitor comments posted and make sure they are respectful and appropriate to the topic.
2. Administrator should request a stop date for comments when a topic is time-sensitive.
3. Administrator should create a summary report of comments and any conclusions drawn and record these with the pastor or immediate supervisor, etc.

10.0 Personal Social Media Sites

Personal Social Media Sites are created by an individual to stay connected with family, friends, and interact with the online community—not for the purpose of ministry. Personal Social Media Sites of persons who are not clergy or religious, such as Employees, Consultants, Volunteers or other Church Personnel, should not be used for ministry or for Diocesan business purposes. Such persons should not represent their communications on their Personal Social Media Sites as official communications from the Diocese. However, it is appropriate and encouraged that Church Personnel will use their personal social media sites for evangelization and for sharing information about diocesan events which are open to the public. All ministry or Diocesan business should be conducted through the official Social Media Sites of the entity to which the individual is assigned. Consequently, Personal Social Media Sites should adhere to the following guidelines:

i. The use of diocesan or church logos and trademarks is strictly prohibited.
ii. Photographs shall not offer images of ministry, church personnel or volunteers.
iii. Ensure transparency: no anonymity or pseudonyms.
iv. Do not disclose confidential information or strictly internal Diocese matters.
v. Any Catholic, living out his/her baptismal call, would hold him/herself as a representative of the Catholic Church and a Personal Social Media Site would reflect this.

11.0 Youth and Social Media

Any media can pose dangers to individuals, particularly in a social setting. The technology which allows young people to foster friendships can also lead to cyberbullying and make them vulnerable to predators. It is everyone's responsibility to safeguard our vulnerable populations. Each Diocesan entity should educate its adult and minor members and parents and students about best practices when using social media. This education would remind parents to be aware of the on-line activities of their children. Each school and faith formation program must offer a safe environment program for parents and students.

11.1 Language Confusion

It is essential to maintain appropriate boundaries between young people and ministry leaders.

1. Appropriate boundaries are essential to all who serve in a ministerial role, and are to be observed in regards to social media as well.
2. The role of 'minister' is distinct from 'counselor', 'friend' and 'parent'. One ministering with young people should never take on the role of 'surrogate parent'. For this reason ministers are highly discouraged from 'trolling' social media with the intent of seeking personal details of a young person's life. While on-line statements are not private, it is the parents' role to monitor their child's behavior, and a minister is not to usurp this role. Intentionally monitoring where youth have shared intimate thoughts violates privacy in the same way that it would to read a journal.
3. Any information encountered within social media that creates a pastoral concern in regard to a minor should be immediately reported to appropriate authorities. Parents are to be informed immediately and legal authorities should be contacted as necessary.
4. To protect both adults and youth, ministers communicating with young people should avoid doing so with excessive frequency and at inappropriate hours. This applies regardless of the form of communication utilized.
5. Those serving in ministry are obligated to consistently represent the teachings of the Roman Catholic Church when using social media. To professionally maintain the trust of the church community, all communication is to be a tool of evangelization.
6. Healthy boundaries between youth and adults are essential. To be a 'friend' to a youth in a ministerial role is to be 'friendly' but is not to establish a peer relationship. A minister serves as a mentor and guide, walking with a young person as they journey in faith. Church Personnel are not allowed to be "friends" online with those under the age of 18. (See General Standard 3.4)
7. Church Personnel must say "no" if asked to be a friend on a personal social media site of a parent, student, parishioner or other individual who interacts with them only through this leadership role. (See General Standard 3.4)

11.2 Transparency

It is essential to the nature of ministry that parents/guardians are fully aware of all media being used to keep in contact with their young person for ministerial purposes.

The intent of any communication policy is that we give witness to the Good News in such a way that we create a safe environment for all vulnerable populations, which is open, transparent and involves the parents/guardians of the young people as partners.

It is important that ministry is not used to establish private one-on-one relationships with youth and our methods of communication must reflect this.

Unusual circumstances of a pastoral nature should be documented and shared with the pastor or one's supervisor as soon as feasible. The documentation of any such circumstance should involve a copy of any applicable communication from all types of communication medium.

12.0 What To Do Before Starting A Social Media Site

Any diocesan entity who feels the need to implement a new social media solution must first thoroughly evaluate the application to be certain it includes the functionality to be compliant with diocesan social media policy. The Office of Communications, Information Technology and Instructional Technology is available to assist with the evaluation of these opportunities. Diocesan entities are asked to inform the Diocese of Orlando Office of Communications and Information Technology when a new social media solution is discovered to allow the diocese at large to benefit from new technology that can enhance communication and evangelization.

Diocesan Network Acceptable Use Policy

1.0 Overview

The Diocese of Orlando recognizes that the Network/Internet and other emerging technologies allow authorized users access to immense information globally. The Diocese of Orlando's goal in providing this privilege to authorized users is to promote professional excellence, innovation, and communication. The use of the Network/Internet or other emerging technologies will be guided by the Diocesan Network Acceptable Use Policy (DNAUP). All Diocese of Orlando authorized users are required to sign a written DNAUP and to abide by the terms and conditions of the policy and its accompanying regulations.

2.0 Purpose

The purpose of this DNAUP is not to impose restrictions that are contrary to an established culture of openness, transparency, trust and integrity. Rather, the Diocese of Orlando is committed to protecting its authorized users from illegal or damaging actions by individuals, either knowingly or unknowingly.

These rules are in place to protect authorized users and Diocesan entities. Inappropriate use exposes Diocesan entities to risks including virus attacks, compromise of network systems and services, and legal issues. Anyone with knowledge of inappropriate material/content should report this information verbally and in writing to the IT specialist or the principal, pastor, or lay person in charge of the school, parish or ministry of the Diocese.

3.0 Policy

3.1 General Use and Ownership

1. Authorized users should be aware that the data they create on systems remains the property of the Diocesan entity. Because of the need to protect the network, management cannot guarantee the confidentiality of information stored on any network device belonging to a Diocesan entity.

2. Authorized users are responsible for exercising good judgment regarding the reasonableness of personal use. Authorized users should be guided by diocesan policies on personal use, and if there is any uncertainty, authorized users should consult their supervisor or manager.

3. The Diocese of Orlando recommends that any information that users consider sensitive or vulnerable be encrypted, especially when stored on external media.

4. Authorized personnel may monitor equipment, systems and network traffic at any time. The Diocese of Orlando maintains the right to monitor all network/computer activity derived from or utilized through its resources, whether it is on-line, down-loaded or through printed material.

5. The Diocese of Orlando, through its entities, reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6. Authorized users are advised that a determined individual may be able to gain access to services on the Network/Internet and other technologies which the Diocese of Orlando has not authorized for professional purposes. By participating in the use of the Network/Internet or other technologies, authorized users may gain access to information and communications which the authorized user may find inappropriate, offensive or controversial. Authorized users assume this risk by consenting to the use of the Network/Internet with the Diocese of Orlando.

7. Anyone who removes diocesan equipment from the business location is required to sign the Receipt of Computer Equipment form. This would include employees who require equipment while working away from the office. If equipment is removed for repair the Receipt of Computer Equipment form or appropriate receipt from vendor can be used.

3.2 Security and Proprietary Information

1. Anyone responsible for entering information into a database or have access to database information used by any Diocesan entity, whether clergy, religious, employee or volunteer, must be FBI fingerprinted and background checked and cleared.

2. The appropriate IT authority of each Diocesan entity does everything possible to ensure the Diocesan entity network is properly maintained and adequate security measures are operational. To assist the appropriate IT authority of each Diocesan entity in sustaining this goal, authorized users, through their supervisor, should notify their IT authority when software and hardware modifications are necessary on any Diocesan computer workstation. At no time should a computer be connected to a Diocesan entity network without knowledge of the IT authority of the Diocesan entity.

   At no time should a computer be connected to a Diocesan entity network without the advanced knowledge and approval of that Diocesan entity's recognized IT authority. Connecting computers and peripheral devices not owned by the Diocese of Orlando (unauthorized devices) to a Diocesan entity network is prohibited unless approved in advance. This includes, but is not limited to, personal computers, printers, flash drives or other external storage devices, switches, routers and wireless equipment. Requests to connect unauthorized devices will be evaluated on a case by case basis.

   The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by school confidentiality guidelines. Staff and students should take all necessary steps to prevent unauthorized access to this information.

3. Passwords will be created by each authorized users for their own use, with the exception of students, volunteers, and temporary/contractual personnel. Authorized user passwords shall not be shared. It is the responsibility of each authorized user to keep his/her password confidential. Anyone whose password becomes known to any other person should notify the appropriate authority immediately and a new password will be created. Anyone who becomes aware of anyone else's password should contact the appropriate authority immediately and a new password will be created. Temporary passwords used by students, volunteers or temporary/contractual personnel may be known by the appropriate authority. However, temporary passwords should not be shared. System passwords should be changed quarterly; user level passwords should be changed every six months.

4. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

5. Because information contained on external media is especially vulnerable, special care should be exercised to protect it in accordance to this policy.

6. Postings by authorized users from any Diocesan email address to on-line bulletin boards, forums, chat rooms, web logs ("blogs")" and any other similar non-work-related discussion groups is prohibited, unless it is specifically work related.

7. All hosts used by the authorized user that are connected to any Diocesan Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.

8. Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

9. Whenever sending "blast" e-mails or e-mails to many recipients, use the blind copy (bc) for the recipients to ensure respecting the privacy of each individual address.

3.3 Unacceptable Use

1. A database of subscribers for parish or other Diocesan use can be a useful tool for parish or Diocesan entity distribution of important messages, calendar of events, or other data. The marketplace is full of companies which offer such database opportunities. This type of database can also compromise a person's identity and/or place an individual in danger, if the database is mis-used or shared indiscreetly. No Diocesan entity should create or subscribe to a vehicle by which subscribers, other than authorized personnel such as employees, priests, deacons, religious or those designated at the discretion of the pastor or Diocesan entity head, are given e-mail addresses to communicate with other subscribers. This does not apply to instructional technology or methodology which includes approved, subscriber access for a specific instructional purpose and is monitored for this purpose. This instructional technology should not offer chat or chat rooms separate from the monitored purpose. In addition, the application should NOT without the written and express permission of each subscriber of the database:

- **a.** Offer Chat or Chat Rooms
- **b.** Allow Blogs
- **c.** Require or Request Photos of Subscriber
- **d.** Require or Request Video of Subscriber
- **e.** Ask for Age or Gender of Subscriber
- **f.** Display Subscriber E-Mail Addresses
- **g.** Allow Subscribers Access to Other Subscriber Information

2. The following activities are, in general, prohibited. Authorized users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

a. Under no circumstances is an authorized user allowed to engage in any activity that is illegal under local, state, federal or international law while utilizing the Diocesan entity-owned resources.

b. Authorized users are prohibited from attempting to circumvent or subvert any system's security measures. Authorized users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

c. When an authorized user becomes "unauthorized" by virtue of employment, dismissal, graduation, retirement, etc., or if the authorized user is assigned a new position and/or responsibilities within the Diocesan system, his/her access authorization will automatically be reviewed with the appropriate individual to determine whether continued access is warranted. This person may not use facilities, accounts, access codes, privileges or information for which he/she has not been authorized.

d. System and Network Activities: 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 Diocesan 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 Diocesan 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.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a Diocesan computing asset to access inappropriate or offensive material or to engage in the procuring or transmitting of material that violates Diocesan anti-harassment or hostile environment policies.

7. Making fraudulent offers of products, items, or services originating from any Diocesan entity account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the authorized user is not an intended recipient or logging into a server or account that the authorized user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, creating or propagating viruses, hacking, network sniffing, spamming, pinged floods, packet spoofing, password grabbing, disk scavenging, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to Diocese of Orlando is made.

11. Executing any form of network monitoring which will intercept data not intended for the authorized user's host, unless this activity is a part of the authorized user's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

e. Employee Responsibilities:

1. Privacy: No authorized user should view, copy, alter or destroy another's personal electronic files without permission.

2. Harassment, Libel and Slander: Under no circumstances, may any authorized user use Diocese of Orlando computers or networks resources to libel, slander, or harass any other person.

3. Abuse of Computer Resources: Abuse of Diocese of Orlando computer resources are prohibited. This abuse includes, but is not limited to, the following:

   a. Game Playing: Installing or playing recreational games, which is not part of authorized and assigned job-related activity, are considered unacceptable practices and are prohibited during normal work hours.

   b. Chain Letters: The propagation of chain letters (e-mail), "Ponzi" or other "pyramid" schemes of any type are considered an unacceptable practice and are prohibited.

   c. Unauthorized Servers: The establishment of a background process that services incoming requests from anonymous diocesan employees for purposes of music/radio/video continuous Internet connectivity, chatting or browsing the Internet is prohibited.

   d. Unauthorized Monitoring: An employee may not use computing resources for unauthorized monitoring of electronic communications of other employees.

   e. Private Commercial Purposes: The computing resources of Diocese of Orlando shall not be used for personal or private commercial purposes or for financial gain.

3.4 Email and Communications Activities: Diocesan entities maintain electronic mail systems. These systems are provided by the Diocesan entity to assist in conducting business within the Diocese.

1. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is not allowed.

2. Unauthorized use, or forging, of email header information is not allowed.

3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is not allowed.

4. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam) is not allowed.

5. The electronic mail system hardware is the property of the Diocesan entity. Additionally, all messages composed, sent or received on the electronic mail system are and remain the property of the Diocesan entity. The Diocese, through the appropriate authority, reserves the right to review, audit, intercept, and access all messages created, received or sent over the electronic mail system for any purpose.

6. The e-mail system was created to facilitate operations of the Diocesan entity. It should be used primarily for business purposes, and only incidentally for personal use. Likewise, personal e-mail through such networks as AOL, Yahoo, Gmail, should be accessed on a limited basis.

7. The electronic mail system may not be used to solicit or proselytize for commercial ventures, political causes, outside organizations or other non-job related solicitations.

8. The electronic mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

9. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

10. Notwithstanding the Diocese's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other authorized users and accessed only by the intended recipient. Authorized users are not authorized to retrieve or read any e-mail messages that are not sent to them.

11. Authorized users shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Authorized users should not attempt to gain access to another authorized user's messages without the latter's permission.

12. All authorized users should perform routine maintenance of their mailboxes and delete messages they are no longer using.

13. The appropriate authority should be notified if a user becomes aware of e-mails which violate this policy.

14. When communicating to a minor through any correspondence such as regular mail, e-mail, text or other technological opportunities for correspondence, such as educational programs, etc., the correspondence must be accompanied by a corresponding copy to the parent.

15. It is the responsibility of the minister or entity to collect parent e-mail addresses and monitor correspondence to be sure parents receive notification at the same time a minor notification is sent.

16. All correspondence must be professional in nature and appropriate for the ministry from which it was sent.

17. Each Diocesan Entity must have a registered domain name that provides appropriate identification of the entity. The preferable Top Level Domain (TLD) is ".org" which is appropriate for nonprofit organizations. All domain names must be registered in the name of the Diocesan entity and not be registered in the name of an individual. Domain registrations can be set to "auto-renew" with the registrar. The auto-renew feature will help prevent domains from expiring unintentionally.

18. Business email accounts must only be provided to approved employees. The creation of business email accounts for employees must be approved in writing by the Pastor or Administrator. Temporary employees and interns can be issued an email account that uses the official domain but the email address should be generic in nature and should not identify the person by name. (e.g., receptionist@orlandodiocese.org, intern@orlandodiocese.org, etc.)

19. Business email accounts must use the domain referred to in the paragraph above. Business email should not use generic domains such as yahoo.com, gmail.com, hotmail.com, etc.

4.0 System Back-up(s)

Although system back-ups should be provided by the Diocesan entity as standard operating procedure, it is the responsibility of each authorized user to backup his/her specific

computer workstation data. Depending upon the amount of the individual workstation usage, workstation backups should occur daily.

5.0 Virus Protection

All networked computers must have current virus protection software installed and operational at all times.

6.0 How to Comply With The Children's Online Privacy Protection Rule

In order to provide interactive service, Diocesan entities might collect personally-identifiable information from the users the website. If such information is collected, the user will be informed about this practice. Additionally, if a website is directed to children or if a general audience website collects personal information from children, the Diocesan entity must comply with the Diocese of Orlando on- line privacy policy. The privacy policy is posted on the Diocese of Orlando website, www.orlandodiocese.org.

Digital Media and Correspondence Policy

1.0 Phone Calls to Minors

Calls should be made to a young person's home rather than to their personal cell phone in order to further transparency. If you speak with a parent/guardian, and in hearing the information you wish to share the parent/guardian asks that you contact the young person directly by the young person's cell phone, you may feel free to do so.

1.1 Calls may provide an opportunity to connect with the parents/guardians as well, and this is a helpful point of connection for family and the ministry.

1.2 Phone calls to a young person should be connected to the ministry setting, and again follow the principles of transparency.

1.3 When you are contacted by a young person be sure to observe the principles of transparency and conduct the conversation as an aspect of the ministry and be present to the conversation as a minister.

1.4 For trips off of church property it is appropriate that youth be given the cell phone numbers of the adult leaders to have in case of emergency, e.g. on an excursion to a theme park. It is also appropriate that, after parents/guardians have been informed, youth cell phone numbers are collected for use that day to ensure safety, following the guidelines of transparency.

2.0 Cards and Letters

A consistent practice of acknowledging and affirming achievements in the lives of those within ministry is certainly appropriate, e.g. sending a note to all graduating seniors or to each young person on their birthday. Communication of this type should be completely transparent and appropriate to a ministry setting. In signing your name it is appropriate to include your title and the name of the ministry you serve.

2.1 Within ministry other occasions may arise in which all youth attending an event receive a short note of affirmation in the context of our faith. This might include *palanca* notes on retreat or an affirmation activity within a program or event. Use good judgment in integrating the outlined aspects of transparency into all of your communications with youth.

3.0 E-mail to Minors

Ministry Leaders should not use their personal e-mail account for their ministry work. The parish should provide each minister with an e-mail account for ministry work and a record of this account reflected in directory information. All e-mail correspondence to a minor must be accompanied by a corresponding copy to the parent/guardian. This will require collecting e-mail information from both parents/guardians and teens at the time of registration for a program/event.

4.0 Text Messaging to Minors

Text messaging should follow the guidelines applicable to other forms of communication, including integrating the principles of transparency. Ministry Leaders and ministry team members should avoid private text communication with any minors. Communicating with youth regarding a ministry event should include copying a text message to the parent/guardian or forwarding the text message to the parent/guardian of the youth through e-mail. Communicating with a group of youth through text messaging may be done as long as parents/guardians are included in the text recipients or are sent an e-mail with the content of the text message, e.g. sending out a reflection or scripture of the day to all youth or providing information on an upcoming event.

5.0 Use of Movies Within Ministry

5.1 Showing movies/clips: Parental/guardian consent forms must be completed before showing any portion of a film rated —Rǁ on the Motion Picture Association of America (MPAA) rating scale to high school age students. This impacts film use within all high school youth ministry programs. The title of the film that will be shown, in whole or part, may be included on the overall parental/guardian consent form for a specific event. If this is a specific evening within a youth ministry planned pattern of gathering a specific parental/guardian consent form should be completed.

5.2 No portion of a film rated —R‖ on the MPAA rating scale may be shown to students under high school age. This impacts film use within all middle school youth ministry programs.

5.3. Parental/guardian consent forms must be completed before showing any portion of a film rated —PG-13‖ on the Motion Picture Association of America rating scale to those under the age of 14. This impacts film use within all middle school youth ministry programs. The title of the film that will be shown, in whole or part, may be included on the overall parental/guardian consent form for a specific event. If this is a specific evening within a youth ministry planned pattern of gathering a specific parental/guardian consent form should be completed.

5.3.a *Best Practice*-- Consult the Catholic News Service movie rating guide, found at Consulte él guía de clasificación de películas en Catholic News Service que se encuentra en www.catholicnews.com/movies.htm before deciding whether or not any clip is appropriate for use within a ministry setting. The USCCB rating system will make note of where a film reinforces or detracts from Gospel values. This system will also indicate films which the MPAA finds age appropriate, that are contrary to the faith. It will also point out films with a high level of resonance with moral and spiritual values of our faith.

5.3.b *Best Practice*—Use clips only from films with which you would be comfortable having the young person recommend to their parents/guardian for viewing the complete film.

5.4 Copyright – CVLI Church Video License provides legal coverage for churches and for other ministry organizations to show motion pictures and other audiovisual programs intended for personal, private use only ("Videos"). (Each organization needs to be specifically covered.) Coverage includes playing just a few minutes of a movie all the way up to showing the full-length feature.

10.0 Using Music Within Ministry

Providing people with tools to access media within a Gospel framework is an excellent practice. Use of music written and/or performed by Catholics or music sung by various choirs of the Diocese provide an opportunity to share the Good News and promote the many blends of Catholic hymns and songs which are available. Using music from the popular culture must include a pre-screening of lyrics. Lyrics with obscenities, or that are demeaning to people of a specific gender, race, creed or sexual orientation, are not to be played/broadcast within the ministry setting.

Video & Webcasting Policy

Well over a quarter century ago, Pope Paul VI wrote about modern communications, "The Church would feel guilty before the Lord if she did not utilize these powerful means that human skill is daily rendering more perfect. It is through them that she proclaims "from the housetops" the message of which she is the depositary. In them she finds a modern and effective version of the pulpit. Thanks to them she succeeds in speaking to the multitudes."

The Diocese of Orlando is embracing these modern communication methods to build the Kingdom of God and share the Gospel message via the tools available through internet and video technologies.

This policy will outline the guidelines to follow when recording video and/or streaming video via the internet.

Televising/Streaming the Celebration Mass

The Diocese of Orlando acknowledges the relevant needs addressed in the Guidelines for Televising Liturgy promulgated in 1997 by the United States Conference of Catholic Bishops, "Being a part of the Sunday worshiping assembly is not always possible for all members of the community. Some people have been hospitalized, home-bound, or imprisoned and do not have the opportunity to be physically present with a regular worshiping community."

Watching recorded, televised and webcast liturgies does not satisfy our obligation to gather in person regularly for these celebrations. However, technologies available in current times provide practical alternatives to remain connected in those circumstances where personal attendance is not possible. Furthermore, all diocesan entities are directed to consider the needs of the gathered faithful who are physically present for the events first and foremost. Therefore, all decisions relating to the videotaping and internet broadcast will put the interests of the physically present ahead of the virtually present.

Acknowledging our responsibility to profess the true teaching of the Church, all material presented through the methods adopted by Diocese of Orlando entities will conform to all policies, guidelines, rules and requirements of the United States Conference of Catholic Bishops, the Diocese of Orlando and the direction of our local Bishop.

These parameters are found in a variety of promulgated documents including, but not limited to:
The Church and Internet, Pontifical Council for Social Communications, *February 22, 2002*
Guidelines for Televising Liturgy, USCCB

Diocese Network Acceptable Use Policy for All Parishes, Schools and Entities of the Diocese of Orlando.
Diocese of Orlando Social Networking Policies

These guidelines are important to maintain the spirit of Church policies particularly related to the protection of vulnerable populations, the privacy of our members and the dignity of each individual who may be involved in these social communications either as a producer, subject or recipient.

Therefore the specific adopted guidelines follow.

Webcasting and Videotaping Liturgical Celebrations

Legal Standard: The Diocese of Orlando recognizes the legal standard which regulates the right to videotape and broadcast persons in public situations. Specifically the legal standard provides for the acceptance of individuals to be videotaped or broadcast in places where cameras are plainly visible.

Desiring to fully inform our members, recognizing potential limitations of some persons to be viewed on broadcast or videotape and respecting the privacy of our members, the Diocese of Orlando adopts these additional guidelines.

Webcasting and Videotaping Mass

Notice of Webcasting and Videotaping
Parishes should adopt a specific Mass or Masses which will be regularly Webcast and notice of these Masses will be provided to members at least two weeks before regularly scheduled programming begins. Additionally immediately prior to the start of any liturgy or event begins, an announcement will be made to the congregants/participants that webcasting and/or videotaping will be taking place. This notice also should be included in the written Mass program.

Permission will be deemed granted for large group views. However for individuals and small groups which would be seen in tight frame, releases will be ascertained from the individuals or legal guardian for those under the age of 18 prior to post-editing, broadcast or posting. For example, parental release forms must be executed for Altar Servers, children's choir, and children who are part of the Offertory. Files will be maintained of these releases for a period of four years, then destroyed. This is in line with the Social Communications Diocesan Network Acceptable Use Policy which states: *Parents/guardians must sign permission slips each year for the use of video where children are present.*

Identity of Participants
In particular, the Eucharistic Celebration is one in which participation of the congregants is a key element and should be noticeable in video media. However, we also wish to respect the privacy of congregants and volunteer liturgical ministers. With these thoughts in mind we set forth the following guidelines:

Identification in title graphics:
While names of Priests, Deacons, Religious and other paid members of the Parish Staff may be specifically identified in a title graphic incorporated in the broadcast or post-editing of a video production, the names of individual congregants, and volunteer liturgical ministers will not be used in any title or graphic unless necessary for an event and in that case with the consent of the individual.

Tight Frames (from a lens perspective) and Close Ups:
In general, camera angles which include congregants will be from the back or side. However, the design of facilities does not permit assurance that faces of all congregants will be unrecognizable. However, most congregant frames will be wide or mid angle. Individual close-up views will not be used, unless agreed to by individual participants prior to the beginning of videotaping or broadcasting. For those under the age of 18, parental release forms will need to be signed, per the Diocesan Network Acceptable Use Policy which states:
Parents/guardians must sign permission slips each year for the use of video where children are present.

Protection of Copyright Materials:
Recognizing the limited performance rights accorded to the parish for copyright material including music, we will make good faith efforts to protect the material we use. Specifically, liturgical events will generally be live webcast only. Events post edited for upload will be limited to those portions which do not include copyright materials. i.e. Homilies or other segments which might be recorded for training or catechetical purposes. Again, an exception would be for events where the parish has been engaged to videotape for the private use of the individuals involved. In those cases, the individuals will agree that the recorded materials will not be replicated in any form and that they will hold harmless the parish for any liability charged against the parish. Pre-recorded music will never be inserted during webcast or videotaping of the Mass. Legally obtained and licensed images may be used tastefully. However, it is preferable to use images from the church building and grounds where these images would be useful as such images better emphasize the live presence at Mass.

Furthermore, a disclaimer should appear on the live stream or video webpage that indicates video is the property of a Diocese of Orlando entity and duplication or retransmission without permission is prohibited.

Disclosure that Obligation to attend Mass is not satisfied:
Prior to any webcast Mass, a notice will be posted in the opening inviting the viewer to attend our Masses in person and advising them that watching the live event does not satisfy their obligation as a Catholic to attend Mass in person, celebrating as the gathered body of Christ.

Direction to Liturgical Ministers
Prior to webcasting all liturgical ministers will be made aware of the videotaping and webcasting.

Use of Titles and Graphics
The action within the celebration of Mass should be the primary focus of the broadcast for the web viewer as it is for the congregants present. Therefore titles and graphics should be used tastefully and in a limited manner. Screen graphics and titles may be used during webcast liturgical celebrations. However, their use will be limited to introductory frames, closing frames and title graphics identifying the name and position of the Homilist. Graphics identifying the Homilist shall only be used at the start of the Homily.

Videotaping Other Events

Liturgical events
Liturgical celebrations in the Catholic Church are meant to be public. In some situations, they may be limited to immediate family members and/or close relatives and friends. Depending upon entity policy, the videotaping of such events for the private use of those who take part in the celebration, or for streaming over the internet or broadcast media, or for the purpose of creating keepsake DVDs or downloadable content may be permitted. In these cases, an image release form for all minors must be obtained. Large venue celebrations such as group confirmations or first receptions of the Eucharist usually involve broader parish participation. On such occasions, depending on entity policy, it may be preferable for the entity to hire professional personnel for photography, videography, or other recording and to make that content available to parishioners or other appropriate parties for individual use and/or purchase. In such cases, an image release form for all minors must be obtained.

Other Events
From time to time a diocesan entity may capture videotape during outreach events, social events, between Liturgical events (i.e. in the courtyard), etc. It is imperative that the Parishes recognize the difference between an event where such a videotape would be limited to a large group view and an event where views would include the recognizable faces of congregants and/or participants. Permission to videotape is only provided in the case of videotaping large group views. In such cases, the aforementioned guidelines must be observed. Videotaping an event with small groups or individuals, which would be seen in tight frame (from a camera lens perspective), requires releases from the individuals or legal guardian for those under the age of

18 prior to post-editing, broadcast or posting. This is in line with the Social Communications Diocesan Network Acceptable Use Policy which states: *Parents/guardians must sign permission slips each year for the use of video where children are present.* Files will be maintained of these releases for a period of four years, then destroyed.

Ongoing Discernment

It is recognized that as issues arise and as technologies expand additional guidelines will need to be created so the integrity and spirit of the guidelines already provided are maintained. The intent of all policies is to honor the privacy of our members, the protection of the vulnerable populations and advances the primary mission of the Church.

Conclusion

The Church has a long history of recognizing the importance of social communications in the dissemination of the truth of Jesus Christ. As "these powerful means that human skill is daily rendering more perfect" have grown and become more accessible to the multitudes, the call of the Church to use them more effectively to "proclaim the Gospel from the rooftops" has grown in fervor. However, we also recognize that with these powerful tools, constraint, prudence and caution must be taken to assure that the message of hope and life which is Jesus Christ is not zealously pursued to the point that the message is clouded or lost in the tools and methods which are available. The abuse of these tools is readily apparent and these abuses have rendered visible many of the precautions we must take to assure the integrity of our actions and purpose.

Initiated: August, 2009
Current: October 2016

Social Media Administrator Agreement

This agreement provides the following Diocese of Orlando entity administrator with "designated social media administrator" rights for ministry-related, instructional-based activities.

The administrator assumes responsibility for the creation of the site, the content they post, and for enforcing the Diocese of Orlando Social Communications Policy.

The administrator understands that a violation of this Agreement or the policies incorporated may result in the loss of social media access on behalf of a ministerial leader, and may result in disciplinary action for Diocese of Orlando employees up to and including termination of employment and/or other legal action in accordance with the terms and conditions of the applicable collective bargaining agreement, board policy, and applicable laws.

In addition, the Social Media Administrator agrees:

• The social media site is considered an extension of the diocesan ministry to grow in our relationship with Jesus Christ, lead our fellow brothers and sisters to a new experience of holiness and share God's love to offer a future of hope to all in need.

• All posts will be monitored and reviewed to ensure they contain church appropriate content.

• The administrator shall bring to the attention of the pastor, principal, or Information Technology director any concerns or violations.

Social Media Administrator:_____Date:_____

Pastor/Principal/Director:_____Date: _____

Site Name:_____Example: Facebook

Site URL:_____Example: http://www.facebook.com/orlandodiocese

Describe your purpose for the social media site (Use the other side of the page as needed.)

Indicate your account privacy settings:

❑ Public page (anyone can see the administrative postings)

❑ Open Group (anyone can see the group and postings)

❑ Closed Group (anyone can see the group, posts are private)

(Only administrators can approve requests to join groups, per policy)

Consent Form for Electronic Communication with Minors

In order to ensure utmost transparency and parental involvement, the Diocese of Orlando has created this consent form so that parents and guardians may select how ministry leaders communicate electronically with minors. Any and all digital networking and communication including but not limited to, email, texting, Facebook, Twitter, other Social Networking sites, etc., with parish youth/school/organization will be ministry related and NOT personal in nature, restricted to matter concerning classes, youth ministry events, parish events, school events, athletic/event schedule or registration forms. This form will be filed in a confidential folder for parish/school/organizational use only. The person(s) being authorized to communicate with the minor child is in compliance with the Diocese of Orlando Safe Environment Policy with this parish/school.

Name of Parent/Guardian: _____

Name of Minor Child(ren): _____

Name of Ministry Leader: _____

Name of Parish/School: _____

Approved Parent Communication Methods (Circle all that apply):
Home Phone
Cell Phone (phone/text)
Email
Social Media Account
Other_____(please explain)

Approved Child(ren) Communication Methods (Circle all that apply):
Home Phone
Cell Phone (Phone/text)
Email
Social Media Account
Other_____(please explain)

❑ You may not contact my child(ren) directly.

Signature:_____ Date: _____