Roman Catholic Diocese of Albany
Social Media Use Policy
In Keeping with the Charter for the Protection of Children and Youth
adapted from
"Recommended Technology Guidelines for Pastoral Work with young People"
National Federation for Catholic Youth Ministry 2010

"The desire for connectedness and the instinct for communication that are so obvious in contemporary culture are best understood as modern manifestations of the basic and enduring propensity of humans to reach beyond themselves to see communion with others." Pope Benedict XVI, 2010 World Communications Day

The following directives will herby serve as the standards for electronic media use by pastoral ministry staff and volunteers who work with children and youth. The following must be read and signed off on before ministry can begin. A copy of the signed statement indicating knowledge of these directives will be kept on file in the parish, school or organizational office.

Church and Ministry Websites

- The official organizational logo should appear on the site to distinguish it as the organization's official site.
- Web content must be consistent with the teachings of the Catholic Church.
- Public websites may not contain personal and/or contact information about children and youth.
- Written permission must be obtained prior to posting photographs, or other identifying information for children or youth on websites. Captions may use only first names and the use of pseudonyms is suggested. Written permission document must be retained in parish or organization files as electronic or hard copy.
- A minimum of two adults functioning with an official organizational capacity should have full access to all organizational account/site(s).
- No personal photographs or information of parish, school or organizational staff or volunteers should appear on any page/site.
- Communication with visitors to the site should be done through official organizational e-mail.

Social Networking Websites

- The official organizational logo or standard images must appear on the site to distinguish it as the organization's official site, and not that of a specific person.
- Priests, deacons, religious, lay ecclesial ministers and volunteers should establish separate sites and pages for personal and professional use. Personal pages and information may never be advertised or accessible to children and youth.
- Priests, deacons, religious, lay ecclesial ministers and volunteers who use social networking sites, either for ministerial or personal use, must be vigilant in representing themselves as ministers of the Catholic Church. Anything that could cause scandal e.g. descriptions of inappropriate use of alcohol; use of inappropriate language etc. must be avoided.
- Parents must be informed that a social networking site is being utilized as a standard part of the ministry.
- A minimum of two adults functioning with an official parish, school, and/or organizational capacity should have full administrative access to the account/site(s).

- Both adults must be registered to have e-mail alerts of page activity sent to their official organizational e-mail addresses. This allows for a quicker response time to urgent requests and helps to ensure that all postings are appropriate.
- Friend/connection requests should be initiated by the young people, not the adult representative of the parish, school, and/or organization.
- In photographs of youth activities, youth may not be "tagged," or identified by name in the photograph.
- On the original social networking site, the "no tagging" option be set.
- Because of the potential for family or teen crises, the nature of ministerial expectations or time relevant information, the page should be monitored frequently by official organizational personnel.

E-Mail and Text/Instant Messaging

- Communications should be professional and rendered on behalf of the parish, school, or organization to youth. Use a parish, school, or organizational e-mail account when communicating parish, school, or organizational business. User must identify him or herself using their professional title in addition to their signature.
- Good judgment should always be used with text based communication tools. It must be assumed that all communications are or have the potential to be publicly known. Avoid engaging in postings/communications that could be misconstrued or misinterpreted.
- Parents should be informed of the use of e-mail or instant messaging for communications purposes with minors, and that it is a standard part of youth ministry.
- Priests, deacons, religious and lay ecclesial ministers and volunteers should maintain separate e-mail accounts for professional/church and personal communications.
- Clear guidelines or parameters must be established with regard to times of communication between adults and youth. Those who minister with young people should pre-determine a time-frame when it is too late to take a professional call, except in the case of serious urgency.
- Care should be taken to maintain professionalism and appropriate boundaries in all communication. Do not overstep the boundaries of adult/youth relationships. Avoid any communication which might be construed as having sexual overtones. Do not reply to any such e-mail received from youth; make and keep a copy of any such inappropriate communication and notify and pastor/parish life director/ supervisor. The latter will inform parent(s) or guardian(s) of inappropriate communications.
- E-mail can be misinterpreted. Always double check messages to see if someone reading it might read something into it that is not intended or if your message might be misinterpreted. If you think an e-mail might somehow be misunderstood, do not send it. Do not send messages in haste or when strong emotions are involved.

Blogging

- Professional, ministry based blogs may only be used to promote upcoming events or programs and for the purpose of evangelization and providing resources and information within the ministry setting. Such blogs may not be used to conduct or promote outside business and/or personal activities, and should not divulge any personal information regarding those being ministered to.
- Extreme care should be taken that information regarding personal blogs is not made available to young people.

- Posted information, opinions, references, and resources should reflect the teachings of the Catholic Church.
- Communications should be professional and are being rendered on behalf of the parish, school, or organization to young people. Purposes include: disseminating fliers for upcoming activities, permission/consent forms, calendars, and ministerial updates, posting links and references for faith formation; communicating sacramental preparation information or parent resources; communicating daily Scripture passages, prayers, or spiritual links/resources.
- If youth engage in blogging as a part of an officially sanctioned organizational activity, such activity must be monitored by at least 2 adults. No youth may be identified by name or other personal information, and the content of such a blog must reflect Catholic Church teaching and values.

Online Video and Chat Rooms

- Any use of live streaming or chat rooms that leads to, supports, or encourages exclusive youth-adult relationships is not allowed.
- When posting videos online, extreme care must be taken to protect the privacy of youth, and such videos may only be used to showcase/advertise ministry related events and activities.
- At no time is one-on-one video or chat room interaction appropriate between adults and minors.
- When presenting personal opinions and engaging in chats/discussions, it is essential for pastoral ministers to remember that even on the World Wide Web, others may recognize them as representing the values of the Catholic Church.

Registration Technologies and Securing Private Information

Capturing information on registration forms, surveys, etc. involves a higher degree of technical understanding and implementation than simple websites or blogs. Forms on webpages can use any number of technologies to record and transmit information, and the transmission of that information can be made more or less secure through the technical decisions and requirements used to develop that form. In simplest terms, no sensitive information should be transmitted through basic web interactions ("http://" in the URL). Only secure, encrypted transmissions ("https://" also known as "SSL" or "Secure Sockets Layer") should be used.

Although secure transmissions ("https://") can happen through any web server, most modern browsers will display strongly worded warnings when the identity of the web server cannot be verified (particularly through third party verification services like Verisign or GeoTrust). Therefore, registration processes that will capture sensitive data usually involve the additional expense of securing a third-party secure certificate.

- No sensitive personal information—particularly financial information (credit card numbers, checking account numbers) and secure identifiers (e.g., social security numbers) should ever be transmitted through e-mail, web pages that convert form information into e-mail, or web forms using regular hypertext transmission ("http://" pages).
- No sensitive personal information should be transmitted over SSL ("https://") unless the user can receive assurance that the communication with the server can be verified through third party services (Verisign, etc.)
- If the explanation of these technologies and the recommendations accompanying them are beyond the technical competence of the webmaster or staff person responsible for registration

forms, that should be taken as a sign that the parish or organization should not be creating such forms. Those leaders should contact a technology/web solution provider for assistance.

- The creation and management of secure web forms is to be done only by a qualified individual or web solution provider.
- Handle all financial transactions "in real time;" that is, on a commerce website that can process credit card transactions online, thus assuring that no financial data needs to be communicated to the parish/organization.
- Even if a form will not include financial information, all security protocols described above are to be followed if other sensitive personal data is transmitted (such as social security numbers, passwords, unlisted phone numbers, etc.).
- Acquire a third party secure certificate (for example, Verisign, GeoTrust, etc.) for any web server that will handle SSL ("https://") transmissions.)

For further information visit: Visit nfcym.org/resources/technology/index.htm

Roman Catholic Diocese of Albany
Social Media Use Policy
in Keeping with the Charter for the Protection of Children and Youth

Consent

I _____
Print name

have read the Roman Catholic Diocese of Albany Social Media Use Policy. I understand its requirements and will follow them in the execution of my ministry with children and youth.

_____ _____
Signature Date

This form must be kept on file in a secure location in the parish / school / organization administrative office.