SOCIAL MEDIA IN THE WORKPLACE: WHAT ARE EMPLOYEES TWEETING ABOUT?

PRESENTED BY:

SAMUEL J. NELSON

MEIER, KENNEDY & QUINN
CHARTERED
ATTORNEYS AT LAW

EMAIL: SNelson@mkqlaw.com

SOCIAL MEDIA IN THE WORKPLACE:
WHAT ARE EMPLOYEES TWEETING ABOUT?

PRESENTED BY
SAMUEL J. NELSON

I. Why Manage Social Media?

- It is a significant part of what the outside world sees of your organization.
- Allows an opportunity to manage employee behavior, both online and in the workplace.
- Safeguards proper communications with minors.
- Allows you to remove inappropriate comments from your own pages.
- "*Any company, big or small, needs a social media policy to protect their reputations. Even if their company has no social media presence, their employees may be creating one by virtue of their actions online.*"
  - Aliah Wright
- 79% of adults who use the internet use Facebook; 32% use Instagram; 31% use Pinterest.

II. Employee Misuse of Social Media

A. Public Image, Employee Misconduct, Church Examples

- Employee statements online impact how others see your organization.
- Employee posts can be evidence of other misconduct or performance issues.
- Examples in the church:
  - Bookkeeper posts negative comments about your parish priest or a bishop.
  - Religious Education teacher posts a photo of herself on Instagram, holding an alcoholic drink, appearing intoxicated.

- Music Director creates a Facebook event titled "Sit-in Protest of Fr. Example's decision to [_____]."

- Custodian tells you he has to leave work early to care for his wife who is sick, and then posts a photo of himself at the beach.

- Receptionist posts a comment about sensitive parish financial information.

B. What to Do?

- Educate employees regarding your policies:

  - Employee Handbook

  - *Justice in Employment*

  - Job Description

  - Code of Conduct for Church Personnel

- Consider designating a specific person as your social media manager.

- Educate Employees regarding internet dos and don'ts:

  - Think before you post.

  - General internet etiquette.

  - Don't make comments on behalf of the parish.

    - *Note: you should provide your employees with a person or process to inform the parish of online activity, so that you are aware of online activity, and when necessary a response is made (e.g., social media manager).*

  - If employees mention the parish or their job position in an online post, they should be clear that the opinions they are sharing are their own.

  - Respect the law (including copyright).

- Be aware of church policies, especially regarding public conduct inconsistent with the faith, morals, teachings, and laws of the Catholic Church.

- Do not post sensitive information.

- Discipline when necessary:

  - What policy has been violated?

  - What evidence do you have?

  - Meet with the employee, providing the employee with a real opportunity to be heard.

  - Take action (documenting any disciplinary measures).

III. Employee Communications with Minors

A. Policies – Code of Conduct for Church Personnel

- Typically, there is no reason for employees to have private communications with minors.

- If a private communication is necessary, it should be kept to professional communications, not personal.

- Parents or guardians of minors must be made aware of any private communications.

- Employees should preserve records of any private communications.

B. What to Do

- Educate your employees regarding the Code of Conduct.

- Take prompt action when necessary in circumstances of a breach of the Code of Conduct.

IV. Parish Social Media

- Parish-Sponsored Groups/Pages
    - Monitor all postings.
    - Be an active presence on the page.
    - If a post is offensive or questionable, document the post, delete the comment, and block the user if necessary.
    - Employees should inform administration of inappropriate posts.
    - Follow policies for employee discipline.
- Employee-Managed Groups
    - Require leadership approval of any group that is associated with the parish.
    - Maintain a social media directory, which lists all pages which are authorized and officially affiliated with the parish.
    - Require employees to share login information with administration and to authorize someone in administration to have administrative access.
    - Significant changes in purpose of a group site should be reported to administration (e.g., a site used for your parish festival is now being used by the social justice committee).
    - Keep group sites private whenever reasonable.
    - Employees should treat parish social media space and communication like a professional workplace.
    - Consider requiring a Site Code of Conduct (stating that all posts should be respectful and on-topic, that the parish reviews and will delete any posts it believes to be violating these rules, etc.).
    - Employees are not authorized to speak on behalf of the parish without prior consent by the administration. Employees should make it clear that any opinions or comments they make online about the parish or related programs are their own personal opinions and that the employee is not authorized to speak on behalf of the parish.

BASED ON NATIONAL BEST PRACTICES, THIS MODEL ACCEPTABLE USE POLICY IS INTENDED FOR USE AS A TEMPLATE FOR PARISHES AND SCHOOLS TO DEVELOP THEIR OWN POLICIES. PLEASE EXERCISE RESTRAINT IN MODIFICATIONS. ADOPTION OF A COMPARABLE POLICY TO THIS MODEL IS RECOMMENDED BY THE ARCHDIOCESE OF SAINT PAUL AND MINNEAPOLIS AND CATHOLIC MUTUAL.

Acceptable Use and Responsibility Policy for Electronic Communications
[“(insert name of parish/school) **AUP”]**

All information used in the course and scope of activities for or on behalf of (insert name of parish/school) is an asset of (insert name of parish/school). Electronic information and communications require particular safeguards and impose unique responsibilities on all Users. (insert name of parish/school) maintains a system of information security to protect our proprietary data. Integral parts of this system are the policies, standards and procedures designed for Users. All Users must adhere to these policies, standards and procedures for the complete system to remain viable.

These policies, standards and procedures apply to all (insert name of parish/school) employees and clergy working directly for (insert name of parish/school) who are users of technology (“Users”) for or on behalf of the (insert name of parish/school)

These policies, standards and procedures include, but are not limited to, maintaining data confidentiality, maintaining the confidentiality of data security controls and passwords, and immediately reporting any suspected or actual security violations. (insert name of parish/school) prohibits the use or alteration of (insert name of parish/school) data and/or information technology without proper authorization. All Users have an obligation to protect the confidentiality and nondisclosure of proprietary, confidential and privileged data, as well as personally identifiable information.

1. Definitions

a. Electronic communications systems include, but are not limited to, electronic mail, telecommunications systems including telephone, voice mail, and video, facsimile transmissions, stand-alone or networked computers, intranet(s), extranet(s), the Internet and any other communications systems that may be created in the future.

b. Electronic communications devices include, but are not limited to, regular and mobile telephones (cell phones, smart phones, walkie-talkies), facsimile machines, computers, laptops, electronic notebooks, audio and video equipment, flash drives, memory sticks, media players, and any other communications devices that may be created in the future.

c. Electronic communications materials include, but are not limited to, DVDs, CDs, laser discs, audio and video-tape, audio and visual recordings, films, microfiche, audio and

visual broadcasts, computer operating systems, software programs, electronically stored data and text files, computer applications, emails, text messages, instant messages, and all other downloaded, uploaded, retrieved, opened, saved, forwarded or otherwise accessed or stored content.

2. Electronic Communications Systems, Devices and Materials and Users Covered

a. All electronic communications systems, devices and materials located on (insert name of parish/school) property (the Premises) or belonging to (insert name of parish/school).

b. All electronic communications devices and materials taken from the Premises for use at home or elsewhere.

c. All personal devices and materials brought from home and used on the Premises during regular business hours

d. All personal devices and materials, regardless of where they are situated, that are used in such a manner that (insert name of parish/school) may be implicated in their use

e. All Users of electronic communications systems, devices and materials.

3. Ownership and Control of Communications

a. All systems, devices and materials located on the Premises, and all work performed on them, are property of (insert name of parish/school). These systems, devices, and materials are to be used primarily to conduct official (insert name of parish/school) business, not personal business.

b. The (insert name of parish/school) reserves the right to monitor, access, retrieve, read and disclose all content created, sent, received, or stored on (insert name of parish/school) systems, devices, and materials (including connections made and sites visited) to law enforcement officials or others, without prior notice.

4. Guidelines for Electronic Communications

a. All Users of (insert name of parish/school) communications systems and devices should use care in creating email, text, video, still images, instant, or voice mail messages or in any postings on any social networking site. (See separate document “(insert name of parish/school) Social Media Policy and Protocol”.) Even when a message has been deleted, it may still exist on a backup system, be restored, downloaded, recorded, printed out, or may have been forwarded to someone else without its creator’s knowledge. The contents of email and text messages are the same as other written documentation and cannot be considered private or confidential.

b. Email and other electronic communications are not necessarily secure, and therefore should be treated accordingly.

c. As with paper records, proper care should be taken in creating and retaining electronic records for future use, reference, and disclosure, in accord with (insert name of parish/school) policy.

d. Mass emails or intranet/extranet/Internet postings to "All Employees," “All Parents” and the like must be approved by the appropriate department director or (insert position title) before they are sent/posted.

e. Use of personal electronic communications devices and materials during regular business hours should be kept to a minimum and limited mainly to emergencies.

f. (insert name of parish/school) systems, devices, and materials are not private and security cannot be guaranteed. Passwords and user IDs are intended to enhance system security; not to provide Users with personal privacy. In addition, all Users do not have an expectation of privacy.

g. User IDs and passwords should not be disclosed to unauthorized parties. User accounts are intended to be used only by the assigned party.

h. All information systems that create, store, transmit or otherwise publish data or information must have authentication and authorization systems, as approved or provided by (insert name of parish/school), in place to prevent unauthorized use, access, and modification of data and applications. Systems that transmit or publish approved information that is intended for the general public may allow unauthenticated (anonymous) access as long as such systems do not allow unauthorized posting and modification of the published information.

i. Computer networks must be protected from unauthorized use. Both local physical access and remote access must be controlled.

j. Information systems hardware should be secured against unauthorized physical access.

k. Minors are prohibited from using (insert name of parish/school) systems, devices, or materials unless appropriate permission is given.

l. If any User knowingly communicates privately with a minor as a part of his or her duties for or on behalf of (insert name of parish/school), reasonable steps must be taken to send the minor’s parent/guardian the same communication content, not necessarily via the same technology.

m. All files downloaded from the Internet, all data received from outside sources, and all content downloaded from portable memory devices must be scanned with updated or current virus detection software. Immediately report any viruses, tampering, or other system breaches to (insert position/title).

n. It is the responsibility of Users to ensure that they save important content to an (insert name of parish/school) approved location in accord with (insert name of parish/school) policy.

o. Only certain individuals, identified per (insert name of parish/school) Social Media Policy and Protocol, may post information to social media sites or (insert name of parish/school)'s website(s) as an official representative of the (insert name of parish/school) (See separate document "(insert name of parish/school) Social Media Policy and Protocol")

p. If a User identifies himself or herself or has reason to be identified as a (insert name of parish/school) employee or clergy working directly for the (insert name of parish/school) in any personal posting or distribution of communication, that User must post the following disclaimer: "The views expressed on this site are mine alone and do not necessarily reflect the views of (insert name of parish/school) or the Archdiocese of Saint Paul and Minneapolis."

5. Prohibited Practices

Users of (insert name of parish/school) electronic communication systems, devices, or materials and Users of personal devices and materials on the Premises under circumstances when the (insert name of parish/school) may become implicated in the use may not:

a. Violate any federal, state or local laws or regulations.

b. Violate any archdiocesan codes of conduct, archdiocesan codes of ethics, archdiocesan safe environment or other archdiocesan policies, or policies of (insert name of parish/school), including but not limited to those that apply to communications or the use of information.

c. Post or cause to be distributed any personally identifying information about a person without permission or review by the person or the person's parent or guardian, if the person is under 18, unless required by the User's job duties or assigned responsibilities. Personal identifying information includes, but is not limited to, images, names or screen names; telephone numbers; home or workplace addresses; email addresses, and web addresses (URLs) of social networking sites or blogs.

d. Post or distribute any communications, video, music, or pictures which a reasonable person may consider to be defamatory, discriminatory, offensive, harassing, disruptive, derogatory, or bullying.

e. Post or distribute any communications, video, music, or pictures which are inconsistent with the faith or moral teachings of the Catholic Church.

f. Engage in improper fraternizing or socializing.

g. Engage in pirating or unauthorized copying, acquisition, or distribution of copyrighted, trademarked, patented materials, music, video, or film or upload, download, view, or otherwise receive or transmit trade secrets, or other confidential, private, or proprietary information or other materials to which the User does not have access rights. Regarding copyrighted materials, certain exceptions are given for educational and liturgical purposes. It is the responsibility of the User to determine copyright status

h. Use electronic communications devices for designing, developing, distributing, or storing any works of programming or software unless required by the duties of the job or assignment.

i. Post or send chain letters or engage in "spamming" (sending annoying, unnecessary, or unsolicited commercial messages).

j. Record any telephone, video, or other conversation or communication without the express permission of the other participants to the conversation or communication, except where allowed by law.

k. Arrange for the purchase or sale of any drugs, alcohol, or regulated substances and goods, or participate in Internet gambling.

l. Upload, download, view, or otherwise receive or transmit indecent, sexually explicit, or pornographic material.

m. Make fraudulent offers of products, items, or services originating from any (insert name of parish/school) account.

n. Damage, alter, disrupt, or gain unauthorized access to computers or others' systems; e.g. use others' passwords, trespass on others' folders, work, or files or alter or forward email messages in a manner that misrepresents the original message or a message chain.

o. Give unauthorized persons access to (insert name of parish/school) systems, provide access to confidential information, or otherwise jeopardize the security of the electronic communications systems (e.g. by unauthorized use or disclosure of passwords).

p. Transmit confidential, proprietary, or sensitive information unless the transmission falls within the scope of the User's job duties or assigned responsibilities.

q. Introduce or install any unauthorized software, virus, malware, tracking devices or recording devices onto any system.

r. Bypass (via proxy servers or other means), defeat or otherwise render inoperative any network security systems, firewalls or content filters.

s. Allow any minor to use the (insert name of parish/school) systems, devices, or materials without appropriate permission.

t. Use electronic communications devices or systems to transmit any radio frequency signal that is not permitted and/or licensed by the Federal Communication Commission ("FCC") or that would violate FCC rules or policies.

u. Access or manipulate services, networks, or hardware without express authority.

v. Provide information about, or lists of, (insert name of parish/school) employees, clergy or other propriety information from the (insert name of parish/school) database(s) to outside parties. Certain exceptions to this prohibition may be made with written approval from (insert position title). Mailing addresses should only be provided in hardcopy (in label or other format as appropriate).

6. Consequences of Violations of Electronic Communications Policy

a. Violations of this policy, including breaches of confidentiality or security, may result in suspension of electronic communication privileges, confiscation of any electronic communication device or materials, and disciplinary action, pursuant to Justice in Employment, up to and including termination of employment, canonical review, referral to law enforcement, and other appropriate disciplinary action.