# SOCIAL MEDIA ISSUES IN SCHOOL: LAWS, POLICIES, AND BEST PRACTICES

**PRESENTED BY**
**SAMUEL J. NELSON**

## I. Student Use of Social Media

### A. The Issue

- More students go online today than ever: In a recent poll, 24% of teens reported being online "almost constantly," 92% report being online daily.

- This creates areas of opportunity, and concern, for schools—enhancing and extending the school environment and community, but also additional risk of improper behavior from students.

### B. Laws and Policies

- MN School Student Bullying Laws: Minn. Stat. §121A.031. Not a requirement for private schools to have bullying policy, but best practice.

- Minnesota's Mandated Reporter Law: Minn. Stat. §626.556. If you have reason to believe a child is being neglected, or physically or sexually abused, must immediately report to authorities.

- MN Stat. 121A.29. If your school participates in a school district chemical abuse program, teachers who know or have reason to believe that a student is using a controlled substance while on school premises or involved in school-related activities, must report this immediately to the school's chemical abuse pre-assessment team.

- Acceptable Use Policy

- Student Discipline Policy

- First Amendment, Free Speech Rights

## C. Cases

- *Requa v. Kent Sch. Dist. No. 415*
    - Student made videos of teacher, posted on YouTube, with student making inappropriate comments.
    - Students received suspension.
    - Students sued.
- *Jegart v. Roman Catholic Church of the Diocese of Houma-Thibodaux*
    - FB page, making fun of Bishop and apologetics course.
    - School punished students based on participation. Creator received 9-day suspension, those who "liked" received 1-day suspension.
    - Student sued for racial discrimination.
- *Doe v. Cal. Lutheran High School Assoc.*
    - MySpace page, showed students were in same-sex relationship.
    - School expelled students.
    - Students sued, discrimination.
- Outcomes for all three cases…

## D. What to Do

- Have policies in place:
    - Acceptable Use Policy, Harassment/Bullying Policy
- Ensure your policies are consistent and up-to-date:
    - Internet Usage? School Computers? Online Activity?
    - Off-Campus behavior?

- Apply policies consistently.

- Educate Students:

    - Encourage students to think before they post—whatever you publish will be around for a long time—could it be hurtful to you or someone else now or in the future? How will this make others feel? Could this impact a job application? A college application?

    - Educate students to protect their own privacy—students should be aware of the privacy settings on their social media accounts, and consider whether their want their postings to be public.

    - Sexting: Make sure students know how serious this is! Seems obvious that it is a serious issue; but to students, it often doesn't seem so.

    - Educate bullies: Oftentimes they are unaware of the hurt they are causing.

    - Educate all: Let students know that they can report bullying and who to report it to; remind them throughout the year.

    - Encourage students to be proactive: Don't "like," share, or pass along hurtful messages or photos; speak out against hurtful postings by posting negative comments (e.g. "this is not cool").

- Educate Staff:

    - Recognize the signs of a student being bullied: Be aware of students' emotional state, watch for dropping grades, changes in relationships, groupings at lunch, etc.

    - School staff should be aware of mandated reporting requirements. Have reporting procedures in place (reporting neglect, physical/sexual abuse, chemical abuse).

- When taking disciplinary action:

    - What school policy has been violated?

    - Was the student given notice of the policy?

    - To what extent does the student's behavior affect the school environment?

    - Maintain a clear record of the evidence used to determine a violation.

- Meet with the student, informing of the charges against the student and allowing the student an opportunity to respond.

- Consider whether to discipline for off-campus actions.
  - Pros:
    - Consistent message, holistic approach for students
    - Reduces disruptions
    - More opportunity to educate and protect students
  - Cons:
    - Perception of school overreach
    - Free speech issues
    - Potential for liability (need to ensure policies are clear and followed)
  - If you do, be sure to have a policy in place!
  - Best Practice – Be able to show that either:
    - The misconduct is a continuation of, or has a nexus with, improper conduct that occurred on school grounds.
      - Does it involve the school itself, students, or employees?
    - The student's actions have a direct and immediate effect on the general safety and welfare of the school community.
      - Is there fear of specific and significant disruption?
      - Is the disruption more than discomfort and unpleasantness, or hurt feelings, from an unsavory viewpoint?
      - Did the student seriously encourage other students to violate laws or school rules?
      - Were teachers unable to control their classes for a significant period of time?

## II. Employee Use of Social Media Related to Students

### A. Laws and Policies

- Family Educational Rights and Privacy Act (FERPA): requires schools to keep student information private, including students' grades, course enrollments, class schedules, etc.
- Children's Online Privacy Protection Rule (COPPA)
- Mandated reporting (both abuse and chemical use)
- Acceptable Use Policy (see attached sample policy for employees)

### B. Liabilities

- Schools that fail to comply with FERPA can lose all federal education funding.
- Failure to comply with federal or state laws allows the harmed individuals to bring a civil lawsuit.

### C. What to Do

- Have a social media policy/acceptable use policy which instructs employees on acceptable behavior, including:
    - Employees should not friend or add anyone known to be under age 13 (many social media sites have age limits, and COPPA may require this (e.g., Facebook requires users to be at least 13)).
        - Consider not allowing employees to friend students at all
    - Requirement to not post anything which compromises employee's professional integrity, ethics, or morals as a professional employed by school.
    - Employees may not post images or videos of students on social media sites without prior written parental consent (except for images of students taken in the public arena, such as at sporting events or fine arts public performances, where the student is not singled out in the photo).
    - Employees may not publicly discuss students or their families outside of school-authorized communications.

- Employee Communication with Students:
    - Communications should be for professional reasons only.
    - Make certain that parents or guardians are aware of the content of any private electronic communications sent to, or received from, a minor.
    - Take steps to preserve records of private communications with youth.

## III. Your School's Social Media Accounts

### A. Laws

- All laws mentioned above apply and should be considered (FERPA, COPPA, Mandated Reporting, etc.)

### B. What to Do

- RE: Student Privacy Requirements
    - Maintain and use Minor Consent Forms for use of student information (see attached sample consent form).
    - Without parental permission, avoid revealing any student information online—this includes posting photos and simply tagging students in photos!
- RE: Employee Managed School Social Media Groups
    - Require approval for school group page/account (consider requiring a "School Based Social Media Registry" application).
    - Maintain a social media directory, which lists all pages which are authorized and officially affiliated with the school.
    - Require staff to share login information with school administration or to authorize someone in administration to have administrative access.
    - Do not give students full management authorization for school accounts.
    - Advisors of official school clubs should have administrative access to group pages, with authority to review, monitor, and change content.

- Employees should treat school social media space and communication like a classroom and/or a professional workplace.

- Group sites should be made private, unless there is a specific reason to make the site public.

- Significant changes in purpose of a group site should be reported to administration (e.g., a site used to share homework information is now being used to share ideas with a class at a school in another country).

- Consider requiring a Site Code of Conduct (stating that all posts should be respectful and on-topic, that school reviews and will delete any posts it believes to be violating these rules, etc.).

- Employees are not authorized to speak on behalf of the school without prior consent by the administration. Employees should ensure that any opinions or comments about the school or related programs make it clear that the comments are personal opinions and do not reflect the opinions of the school.

- RE: School Pages

  - Monitor what is posted.

  - If post is offensive or questionable, document the post, delete the comment, and block the user if necessary.

  - Use questionable comments as teachable moments, remind offender and their parents of the social media code of conduct, and bullying policy.

  - Inform the appropriate administrator.

  - Do not allow posts which include student record information.

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.

**(Insert name of parish/school) DISCLOSURE, AUTHORIZATION, CONSENT AND RELEASE FOR SOCIAL MEDIA OR OTHER ELECTRONIC COMMUNICATION INVOLVING MINORS**

I am the parent or legal guardian of _____(full name of minor) ("My Child").

I certify that My Child is at least 13 years old.

I have been made aware of the (insert name of parish/school) Acceptable Use Policy for Electronic Communications and the Social Media Policy of (insert name of parish/school).

I authorize staff or other leaders of (insert name of parish/school) ("Staff or Leader") to communicate with My Child electronically, including via social media, text, email and phone in accordance with the Acceptable Use Policy for Electronic Communications. Church Personnel are not required to share non-private communications, such as those sent to youth groups regarding meeting locations or times, or other administrative matters. If any staff or other leaders knowingly communicate 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 to me the same communication content, not necessarily via the same technology.

I acknowledge that to review or receive public communications shared via social media with My Child, I will need to become a fan or follower of the same social media. I understand that communications may be accessible or viewable by others who are also fans or followers of the same social media.

**AUTHORIZATION, CONSENT AND RELEASE FOR USE OF VISUAL LIKENESSES AND ORIGINAL WORKS OF MINORS**

I authorize and consent that (insert name of parish/school) and the Archdiocese of Saint Paul and Minneapolis be permitted to use and publish for general communications, advertising, commercial or publicity purposes, or for any other lawful purpose whatsoever the likeness of My Child and My Child's original work, including video, photographic portraits, pictures, or reproductions, made through any medium, including social or other electronic media, in accordance with the Acceptable Use Policy for Electronic Communications and the Social Media Policy, provided only the first name (not the family name) is identified if any name is used. I hereby release (name of parish/school), the Archdiocese of Saint Paul and Minneapolis, and anyone authorized by (name of parish/school) or Archdiocese of Saint Paul and Minneapolis with such use.

This consent regarding My Child's likeness or original work is valid for one year.

If I choose to rescind my authorization and consent, I agree that I will inform (insert name of parish/school) in writing and that my rescission will not take effect until it is received by (insert name of parish/school). I understand however that it may not be possible to recall any work or photos that have been published prior to receipt of my written rescission.

I have read the above Disclosures, Authorizations, and Releases, have had the opportunity to consider their terms, and understand them. I execute this document voluntarily and with knowledge of its significance.

Parent/Guardian Name (please print):_____

Email address: _____

Address:_____

Phone number:_____

Signature of
Parent/Guardian:_____Date:_____