

**THE ARCHDIOCESE OF SAINT PAUL AND MINNEAPOLIS**

**SCHOOL LAW DAY**

**Friday, October 28, 2011**

**CYBERBULLYING, ACCEPTABLE USE,  
AND SOCIAL MEDIA POLICIES FOR  
STUDENTS**

**PRESENTED BY:**

**DOUGLAS C. FRAZEY**

**MEIER, KENNEDY & QUINN**

CHARTERED  
ATTORNEYS AT LAW

**SUITE 2200, BREMER TOWER  
445 MINNESOTA STREET  
SAINT PAUL, MINNESOTA 55101-2137**

**TELEPHONE (651) 228-1911  
FACSIMILE (651) 223-5483  
E-MAIL: [TWieser@mkqlaw.com](mailto:TWieser@mkqlaw.com)**

**NOTE:** The information set forth in these materials is intended to provide an outline of the law existing as of the presentation date. It is not intended as, nor should it be considered, "legal advice." If you are presented with a specific issue, you should consult with legal counsel.

# Creating Effective Cyberbullying Policies in Schools

# Who is affected by cyberbullying?

- 31% of 12-14 year old children, and 40% of 15-17 year old children.
- 34% of girls and 22% of boys aged 12-14
- 41% of girls and 29% of boys aged 15-17

# Bullying, in general, by school type

- Public versus private schools

School characteristic	Number of students	Not bullied	Bullied	Inside school	Outside on school grounds	School bus	Somewhere else at school
Sector							
Public	22,634,000	67.6	32.4	79.0	23.1	8.3	4.0
Private	1,776,000	69.5	30.5	78.7	20.0	2.4 ‡	‡
Catholic	902,000	69.8	30.2	81.7	20.4	‡	‡
Other religious	435,000	61.2	38.8	85.0	15.4 ‡	‡	‡
Nonsectarian	318,000	78.0	22.0	49.3	25.7	‡	‡

‡ Reporting standards not met. These cells did not meet minimum reporting requirements or the standard error for this estimate is equal to 50 percent or more of the estimate's value.

Source: U.S. Department of Education, NCES 2011-316 (May 2011)  
<http://nces.ed.gov/pubs2011/2011316.pdf>

# Who is engaging in cyberbullying?

- 5% of boys aged 12-14 and 8% of boys aged 15-17
- 16% of girls aged 12-14 and 11% of girls aged 15-17.
- It may be that boys are more likely to engage in, and be affected by, more traditional forms of bullying.

Sources: Beckstrom, Darryn Cathryn, State Legislation Mandating Cyberbullying Policies and the Potential Threat to Students' Free Speech Rights, 33 Vt. L. Rev 283,293-94 (2008).

# How does cyberbullying happen?

- Among 12-14 year old children, 38% in instant-messaging conversations, 30% in e-mail, 24% on a website, 15% via photographs made available through email or websites, 14% in text messaging, and 12% in chat rooms.
- Among 15-17 year old children, 48% in instant-messaging conversations, 36% in e-mail, 35% on a website, 11% via photographs made available through email or websites, 22% in text messaging, and 15% in chat rooms.

# Where does cyberbullying happen?

- Among 12-14 year old children, 63% at home, 30% at school, 26% at a friend's house, 5 % elsewhere.
- Among 15-17 year old children, 75% at home, 30% at school, 24% at a friend's house, 5 % elsewhere.
- So, most of cyberbullying appears to take place outside the school. But what can schools do when the perpetrator, victim, and activity are removed from school grounds?

Sources: Beckstrom, Darryn Cathryn, State Legislation Mandating Cyberbullying Policies and the Potential Threat to Students' Free Speech Rights, 33 Vt. L. Rev 283,293-94 (2008).

Megan Meier

# Megan Meier

- In May 2008, H.R. 6123, the "Megan Meier Cyberbullying Prevention Act" was introduced to amend the CFAA "with respect to cyberbullying." This bill did not pass in the 2007-2008 session, but may be re-introduced.
- But note that cyberbullying is often defined in a way as to restrict it to interactions between minors. See Barnett, Colleen, Cyberbullying: A New Frontier and a New Standard. A Survey of and Proposed Changes to State Cyberbullying Statutes, 27 Quinnipiac L. Rev. 579, 580-81 (2009).
- Lori Drew was an adult. In order to encompass cases like Drew's, statutes that use the term "cyberbullying" must define it in terms that include adult as well as minors. See H.R. 6123 (defining cyberbullying as transmitting "any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior").

# Why is cyberbullying different?

- The identity of the bully is in question
- No need for a size or other power imbalance
- Cyberbullying follows the victim
- Cyberbullying is easier in many ways than traditional bullying

# The hazards of online communication

- The impersonality of online communications frequently lends itself to nastiness
  - “It’s easier to fight online, because you feel more brave and in control. On Facebook, you can be as mean as you want.” New York Times, June 27, 2010, “Online Bullies Pull Schools Into the Fray”  
<http://www.nytimes.com/2010/06/28/style/28bully.html?pagewanted=2>
- The effects of electronic communication can be long-lasting, but so can the communication itself.
  - “Kids deal with meanness all the time and many can handle it. But it never lasts as long as it does now, online.” Id.

# State and Federal Law

- “Megan Meier Cyberbullying Prevention Act” – still just a bill
- FCC mandate affects schools in the E-Rate program
- Minnesota criminal law addresses stalking (including cyberstalking) and harassment generally, but the bar is too high to include most cases of cyberbullying in schools.
- Minn. Stat. § 121A.0695: every school board must “adopt a written policy prohibiting intimidation and bullying of any student. The policy shall address intimidation and bullying in all forms, including, but not limited to, electronic forms and forms involving Internet use.”

# Defining cyberbullying

- Avoid including in the definition the effect cyberbullying might have. E.g., “Cyberbullying is activity . . . which has the effect of: Physically, emotionally or mentally harming a student”
- Avoid reference to intent.
- Avoid reference to traits of the victim
- Use a definition of cyberbullying that can accommodate technological change.
- Do not restrict the definition of cyberbullying to activities on school grounds.
- Simplest may be best: “The use of any electronic means to harass, intimidate or bully, whether on or off school grounds.”

Source: Nancy Willard, Cyberbullying Legislation and School Policies: Where are the Boundaries of the “Schoolhouse Gate” in the New Virtual World?, <http://csriu.org/cyberbully/docs/cblegislation.pdf>

# Check your existing bullying policy and...

- State that cyberbullying is a form of bullying.
- Ensure that it covers students who not only directly engage in bullying, but engage in bullying indirectly by condoning or supporting it.
- Leave the potential consequences open—up to and including expulsion. Leave the factors that the school will consider in determining punishment open as well.
- Ensure that the victim's permission does not justify bullying

# Challenges in enforcing a cyberbullying policy

- Identity.
- Discretion.
- The pervasiveness of technology.
- Searches and seizures
- Generation gap.
- Where there's a will, there's a way.
- Adhering to the traditional "bully" model.

# Education and Enforcement Suggestions

- Build student awareness
- Encourage parental involvement and awareness.
- Educate students about the shortcomings of electronic communication.
- Encourage reporting of cyberbullying
- Inform students that law enforcement has a role to play, particularly where a threat of harm exists.
- Inform students that service providers and websites have a role to play, too.

## <SCHOOL NAME> POLICY AGAINST BULLYING AND CYBERBULLYING

### I. PURPOSE

<SCHOOL NAME> is committed to providing a safe educational environment for its students and teachers. <SCHOOL NAME> acknowledges that it cannot monitor all activities and eliminate all incidents of bullying between students, particularly when one or more of the students involved is not on school property or under the direct supervision of school personnel. The purpose of this policy is to assist <SCHOOL NAME> in its goal of preventing and responding to acts of bullying, intimidation, harassment, violence, and similar disruptive behavior

### II. PROVISIONS

- A. <SCHOOL NAME> expressly prohibits bullying, by either an individual student or a group of students, on school property or at school-related functions. <SCHOOL NAME> also expressly prohibits cyberbullying, regardless of whether such acts are committed on or off school property or with or without the use of school resources. These prohibitions apply to students who directly engage in an act of bullying and to students who, by their indirect behavior, condone or support another student's act of bullying. This policy also applies to any student whose conduct at any time or in any place constitutes bullying that interferes with or obstructs the mission or operations of the school or the safety or welfare of the student, other students, volunteers, or employees.
- B. Apparent permission or consent by a student being bullied does not lessen the prohibitions contained in this policy.
- C. A person who observes an act of bullying or becomes aware of such an act must report it to a teacher. Anyone with any bullying-related concerns may also contact the principal.
- D. Retaliation against a victim, good-faith reporter, or a witness of bullying is prohibited.
- E. False accusations or reports of bullying others are prohibited.
- F. A student who violates this policy shall be subject to discipline for that act in accordance with <SCHOOL NAME>'s policies and procedures. <SCHOOL NAME> may take into account all factors it determines to be relevant. Depending on the circumstances, such factors might include:
  - a. The age, development, and maturity levels of the parties involved;
  - b. The levels of harm, surrounding circumstances, and nature and severity of the behavior
  - c. Past incidences or past or continuing patterns of behavior;
  - d. The relationship between the parties involved; and
  - e. The context in which the alleged conduct occurred

Depending on the level and severity of the offense, discipline may range from positive behavioral interventions to more serious consequences, including suspension or expulsion. Consequences for other individuals engaging in particular acts of bullying may include, but not be limited to, exclusion from school property and events or termination of services or contracts.

### III. DEFINITIONS

- A. For purposes of this policy, “bullying” means deliberate or intentional behavior using words or actions that is intended to cause or that does cause fear, distress, intimidation, or harm. Bullying may be repeated behavior or a pattern of behavior, and it may involve an imbalance of power. Bullying can take different forms, including but not limited to:
- a. Verbal conduct (e.g. using threatening or intimidating language, teasing, or name-calling);
  - b. Social (e.g., spreading rumors, ostracizing or socially excluding others, breaking up friendships);
  - c. Physical (e.g., physical acts and gestures, including hitting, kicking, tripping, theft, damaging property, threatening or intimidating behavior); and
  - d. Cyberbullying
- B. For purposes of this policy, “Cyberbullying” means the use of any electronic means to harass, intimidate, or bully, whether on or off school grounds. “Cyberbullying” is a form of bullying, and provisions of this policy that refer to “bullying” are intended to refer to cyberbullying as well.
- C. For purposes of this policy, “on school property or at school-related functions” means all <SCHOOL NAME>’s school buildings, school grounds, and school property or property adjacent to school grounds, <SCHOOL NAME>’s school buses, <SCHOOL NAME>’s school vehicles, <SCHOOL NAME>’s school contracted vehicles, the area of entrance or departure from school grounds, premises, or school-related trips, functions, activities, or events. While prohibiting bullying at these locations and events, the school does not represent that it will provide supervision or assume liability at these locations and events.

# Acceptable Use Policies (AUPs) for Internet Usage

# What is an AUP?

- A written contract between the school, parents and students governing computer, internet, and intranet usage
- It defines access privileges, rules of online behavior, and the consequences for violating those rules

# Why have one?

- Internet use in the classroom is growing.
- School computer systems should be used in a manner that is appropriate, relevant to schoolwork, and safe.
- “A good policy can help protect school resources, limit liability, and clarify rights and expectations”

# Contents of an acceptable use policy

- Preamble
  - School resources are for educational use
  - Accepting the policy is a prerequisite for use of the school's resources
- Requirements
  - Respect privacy
  - Maintain security
  - Respect intellectual property
  - Respect values of the school

# Contents of an acceptable use policy

- Permissive uses (e.g., installing software with a teacher's permission)
- Consequences for violation
- Supervision and monitoring

# What about younger children?

- See Lawrence J. Magid's "My Rules for Online Safety." Among those rules are:
- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
- I will never send a person my picture or anything else without first checking with my parents.
- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.
- I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

# Suggestions

- Draft an acceptable use policy in the form of a contract, which students are required to sign
- Post the AUP in areas where students have access to technology

## **MODEL ACCEPTABLE USE POLICY INFORMATION TECHNOLOGY RESOURCES IN THE SCHOOLS**

The school's information technology resources, including email and Internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources:

### **Students must**

1. Respect and protect the privacy of others.
  - Use only assigned accounts.
  - Not view, use, or copy passwords, data, or networks to which they are not authorized.
  - Not distribute private information about others or themselves.
2. Respect and protect the integrity, availability, and security of all electronic resources.
  - Observe all network security practices, as posted.
  - Report security risks or violations to a teacher or network administrator.
  - Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
  - Conserve, protect, and share these resources with other students and Internet users.
3. Respect and protect the intellectual property of others.
  - Not infringe copyrights (no making illegal copies of music, games, or movies!).
  - Not plagiarize.
4. Respect and practice the principles of community.
  - Communicate only in ways that are kind and respectful.
  - Report threatening or discomfoting materials to a teacher.
  - Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
  - Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
  - Not use the resources to further other acts that are criminal or violate the school's code of conduct.
  - Not send spam, chain letters, or other mass unsolicited mailings.
  - Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

### **Students may, if in accord with the policy above**

1. Design and post web pages and other material from school resources.
2. Use direct communications such as IRC, online chat, or instant messaging with a teacher's permission.
3. Install or download software, if also in conformity with laws and licenses, and under the supervision of a teacher.
4. Use the resources for any educational purpose.

**Consequences for Violation.** Violations of these rules may result in disciplinary action, including the loss of a student's privileges to use the school's information technology resources.

**Supervision and Monitoring.** School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any

student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

**I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS:**

_____	_____
Student	Date
_____	_____
Parent/Guardian	Date

**PARENTS, PLEASE DISCUSS THESE RULES WITH YOUR STUDENT TO ENSURE HE OR SHE UNDERSTANDS THEM.**

**THESE RULES ALSO PROVIDE A GOOD FRAMEWORK FOR YOUR STUDENT'S USE OF COMPUTERS AT HOME, AT LIBRARIES, OR ANYWHERE.**

**FOR MORE INFORMATION, SEE [www.cybercrime.gov](http://www.cybercrime.gov).**

# Social Networking Policies for Students

# What is social media?

- The use of electronic means to create online group interaction, rising to the level of creating online communities
- What forms does it take?
  - Website (e.g., MySpace, Facebook)
  - Blog
  - RSS feed
  - Instant Messaging
  - Message boards
  - Twitter
  - Others

# The Challenges of Social Networking

- Whether or not access to social networking is allowed in the workplace, it can blur the lines between personal and work life.
- Should supervisors associate with (e.g., “friend”) subordinate employees online? Should teachers associate with students online?
- What is said about the workplace (or students, or parents) in online social media is not completely private.
- Social networking on the job may reduce productivity, and is possible even without access to a computer (e.g., smartphones)
- Employees and students may have an inflated expectation of privacy and anonymity.
- Photographs—real or manipulated

# The Benefits of Social Media

But, collaborative social media (wikis, blogs, etc.) can be very useful in classroom group projects or in extracurricular activities.

Social media can be used to broadcast messages to students, families, and employees.

Social media can also be useful in encouraging and facilitating collaboration among teachers, staff, etc.

# What issues does a social networking policy address?

- Protecting Business reputation
- Preventing Breach of confidentiality
- Preventing Student fraternization
- Protecting Whistleblowing
- Limiting Employer liability
- Preventing Plagiarism
- Preventing time-wasting and goofing off

# Social media policies for school employees

- Leverage existing policies.
- A social networking policy can set forth the expectations for conduct.
- Preserving privacy and confidentiality
- Act professionally with regard to students, parents, and others
- Respect copyright laws—including use of the school's logo
- A separate policy for social networking might be needed to address:
  - Posting in online forums.
  - Blogs

# But what about off-duty usage?

- Balancing employees' rights to engage in certain off-duty activities with their employers interests in prohibiting them from doing so.
- Protection of off-duty activities is limited in Minnesota. See, e.g., Minn. Stat. §181.938 (prohibiting discharge of employees, or refusal to hire, for consuming lawful products). Compare to California or North Dakota, which offer protection for employees engaged in lawful activities.
- Alan J. Bojorquez & Damien Shores, “Open Government and the Net: Bringing Social Media Into the Light,” 11 Tex. Tech. Admin. L. J. 45, 67 (2009) (“Employees generally have little or no expectation of privacy regarding electronic data, such as e mails, particularly those transmitted through the employer’s network.”)

# A social media policy for students?

- An AUP and a cyberbullying policy should address many of the problems that student use of social media presents
- It may make sense to have guidelines at the ready for use when social media is integrated into the classroom.
- Policy should represent the educational and moral values of the school

# Sample guideline principles

- Seek Truth and Express It
- Minimize Harm
- Be Accountable
- Responsible use of Information

# Why have a social media policy for employees

The words and actions of employees reflect on the employer

The employer wants to protect its interests in such things as confidentiality and intellectual property

An employee's thoughts expressed on a blog or elsewhere could disrupt the harmony of the workplace

A private religious school may also expect its employees to respect the church and its beliefs

# The Pickering factors

- the need for harmony in the office or work place
- whether the government's responsibilities require a close working relationship to exist between the plaintiff and co-workers when the speech in question has caused or would cause the relationship to deteriorate
- the time, manner, and place of the speech
- the context in which the dispute arose;
- the degree of public interest in the speech
- whether the speech impeded the employee's ability to perform his or her duties.

# Suggestions

- Require employees to disclose to their manager if they are operating a blog
- Require employees to include a disclaimer on any such blog
- Invoke the employee handbook—the same principles will often apply

Due to the wealth of new social media tools available to students, student products and documents have the potential to reach audiences far beyond the classroom. This translates into a greater level of responsibility and accountability for everyone. <SCHOOL NAME> realizes the importance of technology and the importance of using technology to collaborate and share in the process of learning. <SCHOOL NAME> also realizes the importance of creating an atmosphere of trust and individual accountability. As a result, <SCHOOL NAME> has developed the following guidelines to help and protect students when participating in online social media activities. Please keep in mind that information produced by <SCHOOL NAME> teachers and students is a reflection on the entire school and is subject to <SCHOOL NAME>'s Acceptable Use Policy.

By accessing, creating or contributing to any blogs, wikis, or other social media for classroom or district use, you agree to abide by these guidelines. Please read them carefully before posting or commenting on any blog or creating any classroom blog, wiki and/or podcast.

## **Social Media Guidelines for Students**

1. Be aware of what you post online. Social media venues are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.
2. Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
3. Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone besides your teachers and parents.
4. Linking to other websites to support your thoughts and ideas is recommended. However, be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.
5. Do your own work! Do not use other people's intellectual property without their permission. **It is a violation of copyright law to copy and paste other's thoughts.** When paraphrasing another's idea(s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.

6. Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image or it is under Creative Commons attribution.
7. How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
8. Blog and wiki posts should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work be sure it is in the spirit of improving the writing.
9. If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.
  
10. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or access to future use of online tools.

Adapted from <http://socialmediaguidelines.pbworks.com>

# My Rules for Online Safety

I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

I will tell my parents right away if I come across any information that makes me feel uncomfortable.

I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

I will never send a person my picture or anything else without first checking with my parents.

I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.

I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

-- from *Child Safety on the Information Highway*

by Lawrence J. Magid  
(c) 1998 National Center for Missing and Exploited Children