



Office for Protection of Children

1229 Mt. Loretta • P.O. Box 479 • Dubuque, Iowa 52004-0479
Phone (563) 556-2580 FAX (563) 556-5464
Email: dbqcopec@arch.pvt.k12.ia.us

Practical Strategies to Protect Your Family's Social Media Presence

Adapted from an article by Sameer Hinduja, Ph.D.

For better or for worse, social media is an integrated part of today's society. Each one of us has the opportunity to use social media wisely, without compromising our safety, privacy or reputation. Parents should be mindful that their children need to be taught how to interact appropriately online. The following strategies are practical ways that you and your children can improve your social media presence and protect yourselves.



Do not post or send anything you would be embarrassed for certain others to see. Think about what your family, friends or future employers might think if they see it. How would you feel if that statement or picture was forever tied to your name and your identity? Does it really represent who you are? Remember, your keyboard may have a "delete" button, but once online it is often impossible to remove.

Do start early in building a positive online reputation. From the very first post you make on a new social media platform, think about how others will perceive and interpret what you share. Also, actively involve yourself in many positive activities. Get yourself featured in newsworthy projects. Figure out the best ways to create and maintain an online identity that strongly demonstrates integrity and maturity.

Do not compromise your identity. Identity thieves are constantly looking for new ways to obtain your personal information, usually for the purpose of benefiting financially at your expense. Never post your address, date of birth, phone number, or other personal contact information anywhere on social media. Even with restrictions, access can be gained through fraudulent means such as by phishing, hacking or malware.

Do be considerate of others when posting and interacting. If you message someone and they do not respond, or if someone messages you and asks that you not post about them, take the hint and move on. Also do not post pictures of others without their permission. And if someone asks you to remove a picture, post, or to untag them, do so immediately.

Do not vent or complain—especially about specific people or organizations, in public spaces online. People will negatively judge you based on your attitude, even if your complaint has merit. Employers, schools and others have access to social media, and they are looking. Is that spiteful comment about your boss or co-worker really worth losing your job over? Be careful, too, about complaining in seemingly private environments or sending direct messages to others you think you can trust. You just never know who might eventually see your correspondence or posts.

Do properly set up the privacy settings and preferences within the social media apps, sites and software you use. Use the features within each environment to delete problematic comments, wall posts, pictures, videos, notes and tags. Do not feel obligated to respond to messages and friend/follower requests that are annoying or unwanted. Disallow certain people from communicating with you or reading certain pieces of content you share, and allow access only to those you trust. Turn off location-sharing, and the ability to check-in to places. If you need to let your friends know where you are, just text them using your phone rather than sharing it with your entire social network.

Do not post or respond to anything online when you are emotionally charged up. Step away from your device. Close out of the site or app. Take a few hours, or even a day or two, and allow your brain some downtime to think through the best action or response. Responding quickly, based on emotion, almost never helps make a problem go away, and often makes it much worse. Pause before you post!

Do secure your profile. Use complex passwords that consist of alphanumeric and special characters. Avoid using recovery questions that have easy-to-guess or common answers, such as a pet's name. Never reveal your passwords to friends or family, or leave them written down somewhere. Avoid accessing your online profile from devices that are unsecure (like at a library computer), or do not have virus and malware protection.

Do not tell the world where you are at all times. Burglars use social media to target victims by reading posts that clue them in as to where you are (and when you are not at home). Checking in while on vacation or posting an update such as "At the beach for the day" or "Be back in town on Tuesday" may be a fun way of letting your friends know what you are up to, but it also lets those with bad intentions know when your home is empty and vulnerable.

Do regularly search for yourself online, just to see what is out there. Start with Google, but also use site-specific search engines on social networking sites, as well as sites that index personal information about Internet users. Some examples are: peekyou.com, zabasearch.com, pipi.com, yoname.com, and spokeo.com. If you do find personal information about yourself, investigate how you can have it deleted. Many sites provide some type of "opt-out" form that allows you to request its removal.

This article is the copyrighted property of National Catholic Services, LLC (National Catholic), all rights reserved, and is reprinted here with National Catholic's permission. It originally appeared on the VIRTUS Online™ risk management website at www.virtus.org. For more information about VIRTUS Online or other VIRTUS products and services, call 1-888-847-8870.