International Association of
Chiefs of Police

Facebook Safety for Law Enforcement

With over 500 million users worldwide, Facebook is being used by people from all walks of life, including law enforcement officers, defense attorneys, and criminals. Information posted on Facebook and other social media sites may be used in the hiring process, in an internal affairs investigation, or by a defense attorney at trial. Content posted on these sites has been used to disqualify candidates, discipline employees, and impeach officer testimony. Therefore, it is important for law enforcement officials to understand how Facebook works and how to use it responsibly. Below are some things to keep in mind when using Facebook or other social media platforms.

Posting a picture

- What are you doing in the picture? Could it be construed as inappropriate, unseemly, or illegal? Are you engaged in official police activity that could be considered an open investigation or violation of policy if posted?
- Who are you with? Are you with other officers, minors, or others who may not want to be pictured online?

Making a comment

- Could your comment be considered racist, sexist, or otherwise discriminatory or derogatory toward a particular class or individual?
- Does your comment reflect negatively on your agency or coworkers?

"Liking" a cause or organization

- A link to this page will now be placed on your profile, and others who visit this page may see your picture and a link to your profile.
- Are you sure you want to be directly associated with this cause or organization?

"Friending" someone

- Do you know this person?
- Do you trust this person with your personal information?
- Could a link to this person negatively affect your role as a law enforcement officer?

Other considerations:

- Are you undercover or do you hope to have an undercover position at some point?
- Are you revealing your status as a law enforcement officer?
- Are you revealing personal information that could endanger you or your family?

Things you should do:

- Use a strong password. Your password should be at least eight characters long and should contain a variety of numbers, symbols, and letters.
- Check your privacy controls. You can control who sees your information. Most information can be seen by Everyone, Friends of Friends, or just Friends, but you must choose which category of individuals will be allowed to see this information. You can also create custom settings. Set your controls and check them periodically.
- Disable the search engine feature. To prevent people from easily finding you by typing your name in a search engine, disable the feature that allows your profile to come up in search results.

Things you should <u>not</u> do:

- Post your child's name in photo tags or captions.
- Post your entire birth date, address, or phone number.
- Mention that you will be away from home.
- Permit children to use Facebook unsupervised.

REMEMBER, anything you put online could potentially become public no matter how tight your privacy controls. Would you want your mother or father to see this? How about a defense attorney? What about your supervisor?

In September 2010, Interpol chief Ronald Noble became a victim of identity theft . . . on Facebook. The impersonators used Noble's Facebook profile to obtain information on a recent Interpol operation. Facebook fraud can happen to anyone. It is important to take precautions to protect yourself and to ensure that you verify who you are communicating with in cyberspace.

International Association of Chiefs of Police

1-800-THE-IACP
socialmedia@theiacp.org
www.IACPsocialmedia.org

November 2010

This project was supported by Grant No. 2009-MU-BX-K025 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, the Community Capacity Development Office, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document do not necessarily represent the official positions or policies of the U.S. Department of Justice.