

Public Affairs Branch

Personal Use of Social Media Policy and Guidelines

August 2011



NSW Police Force

Table of Contents

1.	INTRODUCTION	3
1.1	Social Media and the Police Force.....	3
1.2	Scope.....	4
Part 1: Policy		
2.	PERSONAL USE AND POLICE EMPLOYMENT	4
2.1	Public Comment and Police Employment.....	4
2.2	Confidential Information	6
2.3	Conflicts of Interest	7
2.4	Monitoring	8
Part 2: Guidelines		
3.	PROTECTING YOUR PRIVACY AND SAFETY	9
3.1	Nothing is Private on the Web	9
3.2	On-Line Friends	12
4.	PROTECTING YOUR CAREER & COLLEAGUES.....	13
4.1	Social Media Use and Your Career	13
4.2	Social Media Use and Covert Careers.....	14
4.3	Protecting Your Colleagues	15
5.	RELATED POLICIES	16
5.1	NSW Police Force Policies	16
5.2	Other Documents.....	16

Title: Personal Use of Social Media Policy and Guidelines
Subject Policy and Procedures
Command responsible: Public Affairs Branch
Available to: All NSW Police Force employees
Authorisation: Commissioner of Police
Publication date: August 2011
Current version number: 1
Review date: August 2013

Copyright of this document is owned by the State of New South Wales through the NSW Police Force © 2011. All rights reserved.

1. INTRODUCTION

1.1 Social Media and the Police Force

The growing popularity of social media creates a new set of opportunities, challenges and risks for the NSW Police Force and its employees. This document seeks to assist police employees to harness the benefits while minimising the risks of social media.

This document should be read in conjunction with the *Media Policy* and the *Code of Conduct and Ethics*.

1.1.1 Defining Social Media

Social media are a group of web-based applications that enable the creation and exchange of user-generated content. Social media occur in a variety of formats including chat rooms, weblogs, social blogs, wikis, microblogging, internet fora, podcasts, pictures, video, and rating and social bookmarking. Examples of social media include, but are not limited to Facebook, LinkedIn, MySpace, YouTube, Flickr and Twitter.

1.1.2 Personal Use

Whether on or off duty a police employee's conduct will reflect on the NSW Police Force. All employees must protect the reputation of the NSW Police Force through behaving in a lawful and appropriate manner¹.

This policy sets standards that must be followed when NSW Police Force employees use social media in a private capacity, especially if they identify themselves as NSW Police Force employees either directly or as part of a user profile, or if they can be identified as working for the NSW Police Force via the content of their postings.

These Guidelines also identify the key dangers involved in the personal use of social media by police employees, and provide recommendations to help employees protect their privacy and career, as well as the safety of themselves, their family and colleagues.

1.1.3 Official Use

Policy on official NSW Police Force social media sites, and on representing the NSW Police Force on-line at police and other social media sites, is set out in the *Official Use of Social Media Policy*.

¹ *Standards of Professional Conduct*, Professional Standards Command, 2009, p.5.

1.2 Scope

This document applies to the personal use of social media sites by NSW Police Force employees². Breaches of the *Personal Use of Social Media Policy and Guidelines* may result in managerial action including loss of confidence or dismissal, and/or criminal or civil sanctions.

This document does *not* apply to the use of social media sites for law enforcement, public information or other official NSW Police Force purposes.

Part 1: Policy

2. PERSONAL USE AND POLICE EMPLOYMENT

2.1 Public Comment and Police Employment

2.1.1 Social Media is Public Comment

There is no such thing as a 'private' social media site, regardless of the privacy settings. Posting information on-line is no different from publishing in a newspaper. If an employee makes any comment about the NSW Police Force on a social media site they are making a public comment.

Employees must not, *in their capacity as NSW Police Force employees*, make any official police comment in social media about any incident, police policy or procedure without prior authorisation in accordance with the *Media Policy*.

Corporate Spokespeople are responsible for representing the NSW Police Force externally on matters concerning particular communities, crimes or policing portfolios. The Spokespeople Program, which includes a Social Media spokesperson, ensures there is expertise and a clear and consistent provision of advice and representation to the public on key corporate issues.

2.1.2 Public Comment as a Private Citizen

The *Media Policy* at section 13.1 states that as private citizens, NSW Police Force employees have the right to enter public debates and comment on policing, political, social or any other issue. (For example, police employees have the right to post comments on news stories at a newspaper's internet site, write letters to the editor or call talk back radio.) However, any comment must be made strictly as a private

² Employee: Police Officer, Administrative Officer, Ministerial Employee or Temporary Employee.

citizen and be separate from, and avoid any reference to, employment with the NSW Police Force.

The *Media Policy* further states that you must not refer to your position or profession when expressing an opinion or participating in public debate in a private capacity. Any comments must not be seen to represent the NSW Police Force, or to compromise your ability to serve the Government of the day in a politically neutral manner.

The *Political Affiliations Code of Conduct* states that comment as a private citizen given in writing on the Internet must be signed without any reference to employment with the NSW Police Force.

If employees refer to police related matters in a private capacity on social media sites then they must avoid any reference to their employment by the NSW Police Force. *If staff choose to identify themselves as NSW Police Force employees* either directly or as part of a user profile, or by posting pictures of themselves in police uniform or holding a police badge etc., or using a police email address, then (regardless of any privacy settings) they are no longer commenting in a private capacity and can only comment if authorised to do so.

For example, a person identifiable as a police officer who posts offensive, racist or obscene material while off duty on their personal social media site, could be in breach of the *Code of Conduct and Ethics* in the same way as if they shouted offensive, racist or obscene material in public while in uniform.

It is strongly recommended that police employees (both sworn and unsworn) not identify themselves either directly or indirectly on social media sites as NSW Police Force employees.

2.1.3 On-line Activity

Point One of the *Code of Conduct and Ethics* states that a NSW Police Force employee must behave honestly and in a way that upholds the values and the good reputation of the NSW Police Force whether on or off duty.

In posting to social media sites in a private capacity:

- give an opinion but be clear that it is a personal opinion
- do not comment on, suggest or hint at matters that are or are likely to be currently under investigation. Such action may jeopardise an investigation or trial
- do not post any material that may bring the NSW Police Force into disrepute, or otherwise embarrass the agency
- do not comment on or post NSW Police Force documents that are not publicly available, whether confidential or not. Links or references to documents on official NSW Police Force internet or social media sites are acceptable
- under no circumstance should offensive comments be made about NSW Police Force colleagues. This may amount to cyber-bullying which could result

in managerial action or criminal proceedings for offences under the *Criminal Code Act 1995* (Cwth)

- make sure on-line activities do not interfere with job performance. For example, public comment on a particular NSW Police Force or Government policy or program is inappropriate if the employee is directly involved in advising on, directing the implementation of, or administering that policy or program, *and* the comment could be seen as compromising the employee's ability to do the job in an unbiased manner
- do not use the police email system and do not provide police email addresses on personal social media posts or sites³
- obey the law – do not post any material that is prejudicial, defamatory, libellous, discriminatory, harassing, obscene or threatening, discloses other people's personal information or infringes intellectual property, copyright or a trademark
- do not imply NSW Police Force endorsement of personal views, or imply authorisation to speak on behalf of the NSW Police Force
- do not use the NSW Police Force name to endorse products, causes or opinions
- do not post NSW Police Force insignia. The use of NSW Police Force insignia such as the chequered band or crest without official consent is prohibited under section 203 of the *Police Act 1990*.

2.2 Confidential Information

2.2.1 Unauthorised disclosure

The unauthorised disclosure of confidential information is a significant risk to the NSW Police Force and has serious ramifications for any employee who commits an unauthorised disclosure.

For example, the disclosure of confidential police information by uploading operational material (crime scene photos, in-car video footage, CCTV footage or footage of police training exercises etc) onto social media sites is a serious breach of legislation and policy and may lead to criminal charges being laid against offending employees.

Point 8 of the *Code of Conduct and Ethics* states that an employee must only access, use or disclose confidential information if required by their duties and allowed by NSW Police Force policy.

Section 62 of the *Privacy and Personal Information Protection Act 1998* prohibits the disclosure of personal information about another person which employees gain access to in the exercise of their official functions. This offence carries a penalty of 100 penalty units or two years imprisonment, or both. The uploading of work related photographs or video such as Scene of Crime photos and In-Car Video or CCTV

³ Use of police email or internet access for personal matters is limited by the Email and Internet Policy, and use to make comments in public debates is inconsistent with that policy.

footage would be a breach of this section. Disclosing a person's criminal record may also breach this section.

Clause 75 of the *Police Regulation 2000* requires officers to treat all information which comes to their attention in an official capacity as strictly confidential, and on no account without proper authority divulge it to anyone. This is a serious matter which may result in managerial action and could jeopardise employment with the NSW Police Force.

The unauthorised publication on-line of confidential information such as training videos discloses police methodology to the public. Police employees who provide police methodology to criminals and the media in this way directly compromise the safety of operational police officers.

Employees who are uncertain whether material they have posted on a social media site is a breach of law or policy, are to remove the material immediately and then seek advice from a senior officer such as a duty officer, professional standards manager or Commander/Director.

2.2.2 Promotion of the NSW Police Force – Authorised Disclosure

Police employees, in posting images or information that they feel promotes positive police work, run the risk of inadvertently positing inappropriate, confidential or sensitive material. To avoid any risk employees are encouraged to instead send the images or information to the Digital Media Coordinator, Corporate Communications Unit, Public Affair Branch, for assessment for posting on official NSW Police Force social media sites.

2.3 Conflicts of Interest

2.3.1 Conflict of Interest Policy

The *Conflicts of Interest Policy and Guidelines* states that it is the responsibility of all employees to take reasonable steps to:

- identify and avoid actual, potential or perceived conflicts of interests
- report those conflicts of interest which cannot be avoided, and
- cooperate in their management⁴.

Where a conflict of interest arises due to an employee's social media site or postings, the employee must notify their Commander or supervisor in writing. The commander/supervisor and the employee must manage the conflict of interest to protect the integrity of the employee and the NSW Police Force.

⁴ *Conflicts of Interest: Policy and Guidelines*, Professional Standards Command, 2009, p.3.

2.3.2 Improper Associations

The NSW Police Force *Conflicts of Interest (Improper Associations) Policy and Guidelines* states that NSW Police Force employees must take all reasonable steps to identify and avoid associations with people, groups or organisations that are involved in (or perceived to be involved in) any activity that is incompatible with the NSW Police Force's role to uphold the law⁵.

An employee's association with some on-line groups or individuals could be seen as endorsement of their views. This includes 'liking' groups on Facebook, 'following' groups or people on Twitter, or accepting people as 'friends'.

Association with individuals, activities or social media groups that may damage the reputation of the NSW Police Force must be avoided. Employees must report improper associations in writing to their manager or supervisor and work cooperatively with them to resolve the conflict of interest.

2.3.3 The Media

If an employee is contacted by the media about posts on their social media sites that relate to the NSW Police Force, they must talk to their manager and the Police Media Unit before responding.

If an employee is offered payment to produce a blog or microblog etc for a third party, this could constitute a conflict of interest and/or secondary employment and must be discussed with their manager.

2.4 Monitoring

2.4.1 Reporting Misconduct

If a NSW Police Force employee becomes aware of a social media site or posting that is illegal or alludes to criminal behaviour, the matter should be reported to the relevant Local Area Command or Specialist Command for investigation.

If employees are aware of on-line criticism or complaints about police activities, the matter should be referred to the relevant Local Area Command or Specialist Command like the Professional Standards Command for assessment.

Should an employee become aware of a social media site or posting that generally damages the good reputation of the NSW Police Force, or becomes aware of the site of a police employee that conflicts with this Policy or the *Media Policy*, please advise the Digital Media Coordinator, Public Affairs Branch, during business hours on E/N 53692 or the Police Media Unit after hours on E/N 45101.

⁵ Conflicts of Interest (Improper Associations) Policy and Guidelines, Professional Standards Command, 2010, p.2.

2.4.2 Audits of Social Media Sites

The NSW Police Force will from time to time conduct audits of social media sites to identify breaches of legislation (including the *Privacy and Personal Information Protection Act 1998* and the *Police Act 1990* and regulations) and NSW Police Force policy (including the *Code of Conduct and Ethics*, *Personal Use of Social Media Policy and Guidelines*, *Corporate Branding Policy* and the *Media Policy*).

Part 2: Guidelines

3. PROTECTING YOUR PRIVACY AND SAFETY

3.1 Nothing is Private on the Web

There's no such thing as a 'private' social media site. Posting information on-line is a public activity and no different from publishing information in a newspaper. Employees are advised to not post anything to social media sites that they would not be comfortable with if:

- quoted in the media
- raised in court while they are giving evidence
- asked about by their mother
- having to justify to their boss, or
- viewed by someone they have arrested.

Everything posted or received on a social media site is public property. Once something is published on-line, control of it is lost forever. Search engines can find posts years after the publication date. Comments, even when sent to friends only can be forwarded, quoted or misquoted. Archival systems save or cache information even if deleted. Once it is posted on-line, it cannot be withdrawn.

The terms of service for social media sites apply to whatever is posted on the site. The terms may allow for posted material to be used in ways that the author did not intend, such as being exchanged with third parties.

3.1.1 Safety - Limit Personal Information

The amount of personal information a police employee places on social media sites is a matter of personal choice. However, employees need to be aware of the potential risks involved for themselves and others when making their decision.

Personal social media sites are a potentially serious safety risk to police employees if not carefully managed to protect the privacy of themselves and others. Disclosing too much private information on social media sites makes a person easy to locate

both on-line and off-line. This vulnerability creates a risk of identity theft, fraud, theft, physical attack, stalking, harassment and intimidation.

For example, if an employee's social media profile contains information such as their date of birth and spouse or parents' names, this can give criminals enough information to answer the security questions an institution will ask before giving them access to the officer's financial or other information.

More importantly, the nature of police work exposes police employees to the risk of offenders seeking revenge. Social media sites with easily accessible personal information provide a simple and effective means to locate an officer and their family or friends.

A search of MySpace by a Professional Standards Command researcher in 2009 easily obtained access to the social media sites of many members of the NSW Police Force who had identified themselves as police officers by rank, name, work location and photographs. Some of these sites included their home addresses and the names and photographs of their children, as well as accessible links to friends who were also clearly identified as police officers. By maintaining such sites these officers are unnecessarily exposing themselves, their family and other police officers to risk of harm.

For example, in 2008 a NSW police officer was contacted on his Facebook site by a person he had investigated and charged in relation to a serious armed robbery, during which shots had been fired. The message was "Let's be friends" but the offender had clearly shown his ability to locate the officer.

It is strongly recommended that to protect themselves, family and friends, police staff (sworn and unsworn) should never identify themselves either directly or indirectly as NSW Police Force employees on social media sites.

It is also recommended that employees strictly limit the amount of personal information they post on social media sites. Employees should think seriously about the risks involved to themselves, family, and friends if they choose to include personal information about themselves or others in posts or social media sites, such as names, dates of birth, home or work addresses, private or work email addresses or telephone numbers, relationship status or any other personal information like photographs that may be useful for identity thieves or criminals seeking revenge. It is a good idea to create a separate email address that is used only with personal social media sites.

If staff choose to identify themselves as police employees, it is recommended that they do not post identifying information about their family such as where they live, where they or their partner works or what school their children attend. For example, do not post photographs of home showing the street number, or photographs of private vehicle(s) showing the licence plates.

3.1.2 Privacy Settings

It is recommended that the highest available level of privacy settings be selected to control access to personal information as appropriate. For maximum security, set sharing rights to 'friends only'. Do not become complacent, as privacy settings are no protection against determined hackers.

Check privacy settings when a social media site is redesigned. During redesign privacy setting may have defaulted to a lower level of security, providing public access to profiles.

3.1.3 StalkBook: Knowing Where You Are

It is recommended that employees do not post information about what they are going to do or where they are going to be – as this makes them easier to target. Employees should limit information on movements to where they have been. To guard against burglaries or malicious damage, do not post information that discloses when you are away from home.

Some social media sites with programs such as Foursquare, Gowalla, Facebook Places or SCVNGR offer the ability to reveal to the public a person's exact location in real time, via mobile phones. While this will enable people to locate friends, it can enable criminals to make a very detailed map of a person's habits, as well as identify their exact location at any given time. Criminals will also know when a person is not at home.

If adopting this type of social media service, it is recommended that employees limit to 'friends only' those who can access their location, and make sure they only have on-line friends they can trust.

Smart phones, some digital cameras and many photo sharing applications allow for or automatically 'geotag'. Geotagging adds geographical identification to photographs, video, and SMS messages. Uploading geotagged photographs to social media sites reveals exactly where the photograph was taken. The more geotagged photographs that are uploaded, the more criminals can gain accurate knowledge of an employee's habits including where they live and work. It is recommended that employees disable the geotagging function (location services) on smart phone cameras and never upload geotagged photographs.

It is also recommended that employees think carefully before tagging photographs with details on where it was taken, and limit access to photographs to 'friends only', and carefully screen on-line friends. Do not give criminals access via social media to photographic information that will enable them to determine the location and floor plan of where you work or live, what valuables you own, or which room you children sleep in.

3.1.4 Protect Your Reputation

It is recommended that employees search for themselves on-line. Contact websites that have posted personal or inaccurate information. If the information contravenes

the website's policies they may remove it. On request social media sites like Facebook and LinkedIn may remove the profiles of persons who impersonate others.⁶

3.2 On-Line Friends

3.2.1 Friends

An employee's safety and on-line security is only as good as their friends' integrity, common sense and security settings.

Professional Standards Command research found that one tactic used by people seeking to obtain confidential information about someone is to simply try to be accepted on-line by their target as a friend. If accepted, they then had access to considerable personal information about their target, including pictures, contact information, lifestyle, family and associates.

Once accepted a friend has the ability to forward to others the private information they have been given access to, or to quote you when they make comments publicly on-line. Given this risk, consider carefully before accepting as a friend a person who works in the media. As other NSW Police Force employees have found, some members of the media will use their on-line friends as a source of information for news stories.

To avoid revealing personal information to strangers, or having inappropriate or illegal postings on a personal site, it is recommended that employees check all potential friends carefully before approving them, especially strangers. Find out if any current friends know the person, and run an on-line search and check their profiles. Only accept people as friends after confirming their identity and that the friendship would not be an improper association. If an employee has any doubts about whether to approve someone as a friend – do not approve them.

Friend profiles should be reviewed occasionally to see if their recent activity is unacceptable or creates a new conflict of interest or improper association.

3.2.2 Friends of Friends

Accepting a friend will also link an employee to that new friend's associates (Friends of Friends). This link, although indirect, can create risks. It is recommended that employees set their privacy settings so that their site cannot be seen by Friends of Friends. (Be aware that the standard setting usually allows access to Friends of Friends.)

For example, at one NSW country Local Area Command, a conversation on Facebook between two police employees included criticism of a work practice. The privacy setting of one of the employees allowed Friends of Friends access, and one

⁶ *Privacy Matters: Social Media, Risk and Reward*, Hub International, September 2010, p.13

Friend of a Friend was a journalist. The criticism was printed on the front page of the local newspaper.

Becoming linked to a friend's associates can also create a conflict of interest with a police employee's public role, or an improper association, which will need to be identified, reported and managed (see section 2.3).

4. PROTECTING YOUR CAREER & COLLEAGUES

4.1 Social Media Use and Your Career

4.1.1 Inappropriate Photographs or Comments

Inappropriate photographs or comments on social media sites are a risk to both the police employee and the NSW Police Force.

Employees are advised to ensure that what they post today will not come back to affect their career, sometimes years later. Choose profile photographs and avatars with care. Employees should think very carefully about the comments they post on-line; especially if intoxicated. It is recommended that employees only do or say on-line what they would do or say off-line in public. For example, staff should only load comments or photographs onto social media sites that they would be comfortable with seeing on the front page of a newspaper.

Reporters and lawyers regularly check the social websites of people who come to their attention. Major newspapers employ staff to actively investigate social media sites to identify content or angles for news stories.

In 2007 photographs of London Metropolitan Police officers behaving inappropriately were found on Facebook by a journalist. The resulting highly critical article featured these photographs, some of which identified officers by name. Further media articles followed featuring more photographs and comments posted by police officers, bringing the individual officers and the London Metropolitan Police into disrepute.

Newspapers generally keep copies of all photographs they publish. The London Metropolitan Police officers identified by their embarrassing photographs may find the pictures re-published by the newspaper years later if they again make the news. This risk may limit their ability to be considered acceptable for any high profile or senior police positions.

It is becoming common for defence lawyers to look for compromising pictures, comments or 'likes' on police officer social media sites. Police officers who put inappropriate content on social media sites can expect to have to defend their reputation at court. For example, to damage the credibility of a NSW police officer who was a prosecution witness in an assault trial, the defence lawyer tabled a picture taken from the officer's own Facebook site. The photograph presented to the jury showed the male police officer in a very intoxicated state wearing a bikini.

A New York defence lawyer got his client's charge downgraded from carrying a loaded weapon to resist arrest by arguing that the arresting officer planted the gun on the defendant as an excuse for breaking his ribs during the arrest. The lawyer succeeded in damaging the officer's credibility by tabling evidence from the officer's social media sites. On these sites the officer had stated he was devious, watching a film about a corrupt police officer to brush up on procedure, and had posted advice on how to assault people during an arrest.

After the trial the police officer told journalists his internet persona did not reflect his actions as a police officer but "...stupidity on the internet is there for everyone to see for all times in perpetuity. That's the case for me."⁷ Once a police officer's reputation is seriously damaged at court, their ability to succeed in future prosecutions is called into question. A successful career as a detective may no longer be possible.

Employers also conduct internet searches on job candidates before making an offer of employment. A person whose social media profile shows them to be socially irresponsible is less likely to be employed.

4.2 Social Media Use and Covert Careers

4.2.1 Undercover and Surveillance Operatives

The NSW Police Force goes to considerable lengths to protect the identity of undercover and surveillance operatives in covert operations; including the provision of assumed identities and the suppression of public records. Police employees must take great care to ensure that undercover and surveillance operatives cannot be identified on-line.

Undercover and surveillance operatives are strongly advised not to have a personal social media site which identifies them by name, photograph, or employment with the NSW Police Force. For example, facial recognition technology can now increasingly link old and blurry photographs to recent clear photographs to confirm or raise questions about a person's identity.

Undercover operatives who use or are identifiable on social media sites may compromise their safety and ongoing operational effectiveness in the Undercover Program. Should this occur an assessment will be made by the Commander, Undercover Branch, as to their continued deployment in this role. The assessment is to ensure the safety and welfare of undercover officers, as well as the integrity of police operations and methodologies.

Police employees must also consider the consequences when they identify colleagues as police officers on social media sites. There is a real potential to inadvertently endanger the lives of covert colleagues by publishing on social media sites pictures or information identifying them or their employment by the NSW Police Force.

⁷ S Hutcheon and A Ramachandran, Body building cop's day in court turns ugly, Sydney Morning Herald, 13 March 2009

Police employees not currently in undercover or surveillance roles should consider the potential affect of having a social media site on their future ability to perform covert duties. An undercover or surveillance career may be impossible after years of publishing their identity and pictures on social media sites. An undercover or surveillance career may also be impossible if other people have regularly published their identity on social media sites.

4.2.2 Counter Intelligence and Extortion

Law enforcement agencies use social media sites to gather intelligence - so do criminals. Police employees run the risk of criminals using social media sites to befriend them on-line to obtain sensitive information. If a criminal can lure the employee into compromising situations either on-line or off-line, then the employee may be vulnerable to extortion to provide sensitive information.

4.3 Protecting Your Colleagues

4.3.1 Postings of other People

Employees should think carefully before posting pictures or personal information about other police employees. For example, posting pictures of colleagues onto social media sites in what is seen as funny situations may seriously damage their reputations and career, or place their life at risk, sometime years after the posting was made and then deleted. Similarly, an employee's reputation and career may be damaged due to postings about them made by their friends or colleagues.

Under no circumstance should offensive comments be made about NSW Police Force colleagues on social media sites. This may amount to cyber-bullying which could result in managerial action or criminal proceedings for offences under the *Criminal Code Act 1995* (Cwth).

Employees should not post details of private conversations, photographs of colleagues, or tag photographs with a colleague's name without permission. Tagging a photograph can put the person tagged at risk. Employees should not tag colleagues and ask others not to tag them in photographs. If asked, employees should not post information about a colleague, and remove any information posted.

4.3.2 Legal Liability

It is recommended that employees seek permission from the person before making postings about others, especially if the posting is compromising or contains information that identifies them by name, photograph, employment with the NSW Police Force, or where they live. Publishing information about work colleagues without first getting their consent may be a breach of the *Privacy and Personal Information Protection Act 1998* or *Health Records and Information Privacy Act 2002*.

A publication which damages the reputation of a person may be defamation. Placing inappropriate pictures of or comments about others onto social media sites, or

allowing others to post such pictures or comments on a personal site, could result in expensive litigation for defamation.

5. RELATED POLICIES

5.1 NSW Police Force Policies

Police policies related to this policy are set out below:

- *Code of Conduct for Police Service Employees and Political Affiliations*, Strategic Development Unit, 2001
- *Conflicts of Interest: Policy and Guidelines*, Professional Standards Command, 2009
- *Conflicts of Interest (Improper Associations) Policy and Guidelines*, Professional Standards Command, 2010
- *Corporate Branding Policy*, Public Affairs Branch, 2007
- *Email and Internet Policy*, Professional Standards Command, 2009
- *Internet Content Policy*, Public Affairs Branch/BTS, 2008
- *NSW Police Force Media Policy*, Public Affairs Branch, 2010
- *Police Notice 08/01: Use of social networking websites such as YouTube and MySpace by NSW Police Force employees*, Professional Standards Command, 2008
- *Standards of Professional Conduct* (which includes the *Code of Conduct and Ethics*), Professional Standards Command, 2009.

5.2 Other Documents

Other documents related to this policy are set out below:

- *Body building cop's day in court turns ugly*, S Hutcheon and A Ramachandran, *Sydney Morning Herald*, 13 March 2009
- *Circular 2008/8: Interim protocols for online media participation* Australian Public Service Commission, 2008
- *Designing Social Media Policy for Government: Eight Essential Elements*, University of Albany, 2010
- *Privacy Matters: Social Media, Risk and Reward*, Hub International, September 2010
- *Intelligence Research Report*, Professional Standards Command, 2009
- *Internet-Intranet Usage Policy*, Museum of Applied Arts and Sciences, 2010
- *Social Media - Telstra's 3 Rs of Social Media Engagement*, Telstra, Public Policy and Communications
- *Social Media Policy and Law Enforcement*, GoverningPeople.com, L, Stevens, 2010.