New South Wales
Police Force

Personal Use of Social Media Policy and Guidelines

Public Affairs Branch

14 August 2015

Unclassified

Personal Use of Social Media

This policy applies to the personal use of social media by NSW Police Force employees, and seeks to assist staff to gain the benefits while minimising the risks.

Essential Summary

Posting as a Private Citizen

When posting on social media sites in a private capacity, NSW Police Force employees must behave in a way that upholds the values and reputation of the NSW Police Force. Employees must not discuss or disclose NSW Police Force information that is not publicly available, whether confidential or not.

If employees comment on police related issues in a private capacity on social media sites, they must avoid any reference to their employment by the NSW Police Force. If staff choose to identify themselves as police employees they are no longer commenting in a private capacity and can only comment if authorised to do so in accordance with the *Media Policy* and the *Official Use of Social Media Policy*.

An employee's association with some on-line groups or individuals could be seen as endorsement of their views. Association with individuals, activities or social media groups that may damage the reputation of the NSW Police Force must be avoided. Employees must report to their supervisor any on-line declarable associations.

Personal Information

It is recommended that employees strictly limit the personal information they post on social media sites. Disclosing too much private information 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.

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

Undercover and surveillance operatives are strongly advised not to have a personal social media site which identifies them by name, photograph or police employment.

Inappropriate photographs, comments or 'likes' on social media sites are a risk to both the police employee and the NSW Police Force, It is recommended that employees only do or say on-line what they would do or say off-line in public.

Friends

An employee's safety and on-line security is only as good as their friends' integrity, common sense and security settings. Make sure your family and friends understand the risks involved. Encourage them to use the highest privacy settings and not identify you as a police employee.

Table of Contents

Document Properties

Title	Personal Use of Social Media Policy and Guidelines
Subject	Policy and Procedures
Command responsible	Public Affairs Branch
Authorisation	Commissioner's Executive Team
Available to	Unrestricted
Publication date	November 2015
Current version number	Two
Review date	June 2017
Document number	
Copyright statement	Copyright of this document is owned by the State of New South Wales through the NSW Police Force © 2015. All rights reserved.

Modification History

Version #	Version approval date	Author/Position	Summary of changes
1	August 2011	Alan Tongs Executive Officer	New Policy
2	27 October 2015	Alan Tongs Executive Officer	Policy revised and updated, especially at sections 2.2, 2.4.3, 3.2, 3.3, 4.1.1 and 4.2.

1. INTRODUCTION

1.1 Context: Social Media and the Police Force

The popularity of social media creates opportunities, challenges and risks for the NSW Police Force and its employees. This document aims to assist police employees gain 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 highly accessible user-generated content. Social media occur in a variety of formats including chat rooms, weblogs, social blogs, wikis, microblogging, internet fora, vod and podcasts, pictures, video, and rating and social bookmarking. Examples of social media include but are not limited to Facebook, LinkedIn, MySpace, YouTube, Flickr, WhatsApp, Twitter, Weibo and Instagram.

1.1.2 Personal Use

Whether on or off duty a police employee's conduct reflects on the NSW Police Force. All employees must protect the reputation of the NSW Police Force by behaving in a lawful and appropriate manner[1].

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.

The guidelines 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 and overt NSW Police Force social media sites, and on officially representing the NSW Police Force on-line at police and other social media sites to engage with the community, is set out in the *Official Use of Social Media Policy*.

1 *Code of Conduct and Ethics (Standards of Professional Conduct Booklet)* Professional Standards, 2013, p.5.

1.2 Scope

This document applies to the personal use of social media by NSW Police Force employees[2]. 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.

2.1.2 Public Comment as a Public Official

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

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

2.1.3 Public Comment as a Private Citizen

The *Media Policy* 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

2 Employee: Police Officer, Administrative Officer, Ministerial Employee or Temporary Employee, and persons engaged to assist the NSW Police Force to undertake its responsibilities in accordance with the *Police Act 1990*.

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

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

If employees comment on police related issues 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 indirectly, such as in a user profile, or by posting or hosting pictures of themselves in police uniform or holding a police badge or using a police email address etc., 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 directly or indirectly identify themselves or their colleagues as NSW Police Force employees, when personally using social media.

2.2 Personal On-line Activity

2.2.1 Posting as a Private Citizen

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 it is a personal opinion
- 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 (such as by liking or recommending products)
- do not comment on, suggest or hint at matters that are or are likely to be currently under investigation or before the courts. 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 disclose NSW Police Force information that is not publicly available, whether confidential or not. Links or references to

information on official NSW Police Force internet or social media sites is 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[3] 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 fulfil their duties in an unbiased manner
- do not make comments so harsh or extreme in its criticism of the Government, a member of parliament, a political party, or their policies, that it raises questions about the employee's capacity to work professionally, efficiently or impartially. Such comment does not have to relate to the employee's area of work
- do not use the police email system and do not provide police email addresses on personal social media posts or sites
- obey the law – do not post any material that is prejudicial, defamatory, bullying, libellous, discriminatory, harassing, obscene or threatening, constitutes a contempt of court or breaches a court suppression order, discloses other people's personal information or infringes intellectual property, copyright or a trademark or is otherwise unlawful
- do not post pictures of NSW Police Force insignia, including the police uniform or ribbon. The use of NSW Police Force insignia such as the uniform, chequered band or logo without official approval is prohibited under section 203 of the *Police Act 1990.*

Employees should understand that even if they do not identify themselves on-line as police employees by posting anonymously, or using an alias or pseudonym, their identity and their employment may later be revealed. In 2013 a Federal Immigration Department employee was dismissed after she was identified as the author of a Twitter account which published comments highly critical of the Government's refugee detention policies.

2.2.2 Misuse of Police Resources: Personal Use while on Duty

The *Use of Resources Policy* states that employees are required to perform their duties with minimum disruption. While limited use of resources for personal reasons is allowed, excessive breaks for non-work related activities, such as accessing social media sites, is considered a misuse of police time.

Any use of a personal or police electronic device to access social media for personal reasons while on duty should be infrequent and brief, not disrupt normal business (e.g. does not interfere with the employee's work responsibilities or the work of others) and not involve activities that might be questionable, controversial or

[3] *Harassment, Discrimination and Bullying*, Human Resources Command, 2007

offensive[4] (such as by breaching section 2.2.1 above). For example, police employees have been subject to management action for accessing and playing games on social media for lengthy periods while on duty.

2.3 Confidential Information

2.3.1 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 such a disclosure.

For example, the unauthorised disclosure of confidential police information by uploading operational material (crime scene photos, in-car video footage, CCTV footage or video 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. Disclosing a person's criminal record may 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 divulge it to anyone without proper authority. 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 the media, or to criminals and terrorists 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 constitutes 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.

4 *Use of Resources Policy*, Professional Standards Command, 2014, s.2.5 pp.7-8, *Information Security Manual*, Business and Technology Services 2014, Ch.10, Obj.8, pp.55-6, and *Email and Internet Guidelines,* BTS, 2012, Sec.4 p.6.

2.3.2 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 posting 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 Affairs Branch, for assessment for posting on official NSW Police Force social media sites.

2.4 Conflicts of Interest

2.4.1 Conflict of Interest Policy

The *Procedures for Managing Conflicts of Interest* state it is the responsibility of all employees to take reasonable steps to identify and avoid actual, potential or perceived conflicts of interests.

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[5].

2.4.2 Declarable Associations

The NSW Police Force *Procedures for Managing Declarable Associations – Individual Responsibilities*, state that 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) activity that is incompatible with the NSW Police Force[6].

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, following channels on YouTube and people or pages on Instagram, 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 declarable associations in writing to their commander/manager and work cooperatively with them to implement an appropriate management strategy.

2.4.3 Secondary Employment

Any personal use of social media to promote secondary employment must not create a conflict of interest between the employee's official duties and the secondary employment, or otherwise breach the *Secondary Employment Policy and Procedures*. See the *Secondary Employment Policy and Procedures* for details.

5 *Procedures for Managing Conflicts of Interest,* Professional Standards Command, 2012, p.12.

6 *Procedures for Managing Declarable Associations – Individual Responsibilities*, Professional Standards Command, 2012, p.3, 8-10.

2.4.4 The Media

If an employee is contacted by the media about posts on their personal 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.

2.5 Monitoring

2.5.1 Reporting Complaints, Misconduct or Illegal Activities

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

Police officers who become aware of actions on social media by other police officers which they believe constitute a criminal offence or other misconduct, are required by clause 49 of the *Police Regulation 2008* to report the matter to a senior officer.

If employees are aware of on-line criticism or complaints about police activities, consider referring the matter 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 45217 or the Police Media Unit after hours on E/N 45101.

2.5.2 Audits of Social Media Sites

Employees should expect that any information they create, post, exchange or discuss etc., on a publicly accessible on-line location may be viewed by the NSW Police Force at any time without notice.

The NSW Police Force may 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 Standards* and the *Media Policy*).

Part 2: Guidelines

3. PROTECTING YOUR PRIVACY AND SAFETY

3.1 Nothing is Private on the Web

There is 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 social media is public property. Once something is published on-line, control of it is lost forever. Search engines can find posts years after publication. 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.

3.2 Safety

3.2.1 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 risks involved for themselves and others when making their decision.

Personal social media sites are a 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 or a terrorist attack. Social media sites with easily accessible personal information provide a simple and effective means to locate an officer and their family or friends.

The Public Affairs Branch conducts social media searches on the names of some employees attending social media training. The social media sites of NSW Police Force members can often be easily located due to staff identifying themselves as police officers by rank, name, work location and photographs in uniform. Some of these sites include home addresses and the names and photographs of their children, as well as accessible links to friends who are 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, one 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.

Be aware that police officers are increasingly being filmed by the public during operational incidents. The footage is then posted onto social media sites, resulting in people seeking to identify the officer to target and harass that person. Posting photographs of yourself, especially in uniform, or otherwise identifying yourself as a police employee on your personal social media sites, makes you very easy to find.

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

It is also recommended that employees strictly limit the personal information they post on social media sites. Employees should think seriously about the risks to themselves, family, and friends if they choose to include personal information in posts or social media sites. Personal information that is useful for identity thieves and criminals seeking revenge includes:

- names
- dates of birth
- home or work addresses
- private or work email addresses or telephone numbers
- relationship status
- photographs of yourself, family or colleagues
- photographs of personal vehicles, home or work location. In particular photographs showing vehicle number plates, street names and house numbers, or the internal layout of your home.

If staff choose to identify themselves as police employees, it is strongly 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.

It is a good idea to create a separate email address that is used only with personal social media sites.

3.2.2 Google Maps and Home Locations

In early 2015 a tag was created on Google Maps publicly identifying a street location as the home of a police officer from the Middle Eastern Organised Crime Squad (MEOCS). Given the risk to officer safety, all employees are advised to regularly check their home location on Google Maps to identify if their residential address has been publicly tagged as the home of a police employee.

If your home has been tagged, advise the Public Affairs Branch by email at #PUBLICAFFAIRS. The Public Affairs Branch will urgently contact Google and arrange for the tag to be removed.

If you park a marked police car on the property at your home there is a risk that it may be photographed by Google Maps street view and published on the internet until such time as the photograph is updated. This risk of having your home location identified on Google Maps is low but real, and has already happened to some police officers.

3.2.3 Contacting Offenders/POIs

Keep your personal use separate from any official use of social media. Do not use your official police profile for personal use. Do not use personal social media sites for official use. In particular, do not contact offenders or persons of interest via personal sites, such as to forward or serve official documents. Employees who identify their personal social media sites to offenders or POIs etc., create a serious safety risk for themselves and their family, and any other colleague or individuals linked to that personal site.

3.3 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’. Also set your Facebook Friends List to ‘Friends’ or ‘Only Me’ as your personal information can often be found by searching your friends’ Facebook pages. Do not become complacent, as privacy settings are no protection against determined hackers.

Check privacy settings regularly, especially 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.

Keep your photographs private. If you do use photograph and video sharing networks like Flickr, make sure you set high privacy and permission restrictions.

3.3.1. StalkBook: Knowing Where You Are

It is recommended that employees 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, such as when you are going away on holidays.

Some social media sites including Facebook and Twitter 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 or terrorists 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.

Similarly, with applications like Map My Run and Strava, if you routinely run at a particular time and location, or if you start and finish at your home address, you can be easily located.

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.

3.3.2 Geotagging and Tagging

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 your children sleep in.

It is recommended that settings which notify a user that they have been tagged in a photograph, and require approval for the tagged photograph to be added to their page, should be turned on. Also, ask friends not to tag you in photographs they post.

3.3.3 Protect Your Reputation

It is recommended that employees search for themselves on-line. You can also consider setting up a Google Alert to send you an email whenever you are mentioned on social media. 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.[7]

3.4 On-line Friends

3.4.1 Friends

An employee's safety and on-line security is only as good as their friends' integrity, common sense and security settings. Make sure your family and friends understand the risks involved. Encourage them to enable the highest privacy settings and not identify you as a police employee.

Professional Standards Command research found that one tactic used by people seeking 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 the 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 a declarable 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 you are still comfortable sharing information with them, plus to see if their recent activity is unacceptable or creates a new conflict of interest or declarable association.

3.4.2 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

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

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 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 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 a declarable association, which will need to be identified, reported and managed (see section 2.4).

4. PROTECTING YOUR CAREER & COLLEAGUES

4.1 Social Media Use and Your Career

4.1.1 Inappropriate Photographs, Comments or Likes

Inappropriate photographs or comments on social media sites are a risk to both the police employee and the NSW Police Force. Liking or following inappropriate comments, sites or groups is equally a risk.

Employees are advised to ensure that what they post, like or follow 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 say or like 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.

Police employees who post inappropriate comments or photographs on social media are regularly subject to formal complaints from members of the public or other police employees. Management action taken against such employees range from formal counselling, warning notices or placement on a Conduct Management Plan, through to loss of increment and dismissal under 181D of the *Police Act 1990*.

For example, a former officer used Facebook to repeatedly post inappropriate and abusive personal comments. The Facebook page had no security settings and it was obvious the person was a police officer. These views were widely circulated until they were brought to the attention of the officer's Local Area Command by a member of the public.

The types of inappropriate posts that have led to complaints, investigations and management action for misconduct include:

- offensive comments about the abilities, intelligence, physical appearance and other personal attributes of colleagues
- negative comments about the competence of management or the NSW Police Force as a whole
- racist or other offensive comments about the local community
- flippant comments that were intended to be humorous, but were offensive to colleagues or the local community
- flippant comments about the use of firearms
- photographs taken off duty that were intended to be humorous but included offensive text, images or symbols
- comments posted while on duty about current work tasks.

Police employees who allow themselves to be photographed by others while acting inappropriately have also been subject to formal complaints. For example, during a New Year's Eve event alcohol affected females asked a male police officer if they could be photographed with him and his police vehicle in an inappropriate pose. The officer consented and the photographs were circulated on Facebook by the females the next day, resulting in management action being taken against the officer.

Reporters and lawyers also regularly check the social media sites 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.

4.1.2 Personal Social Media sites and Reporters

In England, 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.

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.

4.1.3 Personal Social Media sites and Defence Lawyers

It is common for defence lawyers to look for compromising pictures, comments or 'likes' on police officer social media sites. Police officers who post, like or follow inappropriate content such as drunken or obscene comments or images, or express bias against a person's race, religion, sex or ethnic group 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."[8] 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 or police prosecutor 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. All 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. 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.

An *In these Times* article stated that in the United States District of Columbia a protest group identified an undercover police officer who had infiltrated them due to her regular posting of personal information on social media sites, including photographs of herself, an envelope showing her work address, and that she was a police officer currently working in plain clothes. The protest group filed a law suit against the police department and the 'covert' officer became a news story.[9]

8 S Hutcheon and A Ramachandran, Body building cop's day in court turns ugly, Sydney Morning Herald, 13 March 2009.
9 *Activists Identify DC Cop Who Infiltrated Bangladesh Sweatshop Protests*, In these Times, 6 August 2013.

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 the 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 Police Force.

Police employees not currently in undercover or surveillance roles should consider the potential effect 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 and terrorists. Police employees run the risk of criminals or terrorists using social media sites to befriend them on-line to obtain sensitive information. If the employee can be lured 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 Police Employees

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 should remove any information posted.

It is recommended that employees not post personal photographs or any other content that could identify a colleague as a Police Force employee.

4.3.2 Legal Liability

It is recommended that employees seek permission from colleagues before making posts about them, especially if the post 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 onto your personal sites, 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 and Ethics (Standards of Professional Conduct Booklet)* Professional Standards Command, 2013
- *Corporate Branding Policy and Standards*, Public Affairs Branch, 2014
- *Email and Internet Guidelines,* Business and Technology Services, 2012
- *Harassment, Discrimination and Bullying*, Human Resources Command, 2007
- *Information Security Manual*, Business and Technology Services, 2014
- *Internet Content Policy*, Public Affairs Branch/BTS, 2011
- *NSW Police Force Media Policy*, Public Affairs Branch, 2013
- *Police Notice 08/01: Use of social networking websites such as YouTube and MySpace by NSW Police Force employees*, Professional Standards Command, 2008
- *Procedures to Manage Declarable Associations: Individual Responsibilities*, Professional Standards Command, 2012
- *Procedures for Managing Conflicts of Interest*, Professional Standards Command, 2014
- *Secondary Employment Policy and Procedures,* Human Resources Command, 2015
- *Use of Resources Policy*, Professional Standards Command, 2014

5.2 Other Documents

Other documents related to this policy are set out below:

- Activists Identify DC Cop Who Infiltrated Bangladesh Sweatshop Protests, Mike Elk, *In these Times*, 6 August 2013
- 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
- *Circular 2012/1: Revisions to the Commission's guidance on making public comment & participating online*, Australian Public Service Commission, 2012
- *Circular 36*, Police Association of NSW, 8 December 2014
- *Designing Social Media Policy for Government: Eight Essential Elements*, University of Albany, 2010
- *Intelligence Research Report,* Professional Standards Command, 2009
- *Internet-Intranet Usage Policy*, Museum of Applied Arts and Sciences, Sydney, 2010
- *Privacy Matters: Social Media, Risk and Reward*, Hub International, September 2010
- *Social Media Handbook for Police,* Police Association of NSW, 2014
- *Social Media Model Policy,* International Association of Chiefs of Police, 2010
- *Social Media - Telstra's 3 Rs of Social Media Engagement,* Telstra, Pubic Policy and Communications
- *Social Media Policy and Law Enforcement*, GoverningPeople.com, L, Stevens, 2010.
- *What Staff need to know about Social Media and Technology,* NSW Department of Education and Training, undated