information and privacy commission
new south wales

Social Media Policy

March 2015

Table of contents

Acknowledgement: The IPC has drawn extensively on the Department of Justice's Social Media Policy and Social Media Procedures in developing this document. We thank the department for its excellent work.

Introduction

By using social media, government can reach new audiences, establish communities of practice, provide services and deliver important and effective messages to stakeholders.

The NSW ICT Strategy recognises these benefits and encourages widespread use of social media for government business to:

- improve customer services
- increase access to information, and
- involve the community directly in government decision making.

The Information and Privacy Commission NSW (IPC) recognises the value social media provides to business and the community. To leverage this value, social media channels and tools should be well managed.

This Policy has been based on the NSW Department of Justice Social Media Policy, and provides a framework for the creation of social media accounts and ongoing use of social media as a tool for fulfilling business needs where appropriate.

It is to be read in conjunction with the document IPC Social Media Procedures.

This policy will be reviewed annually.

Essential summary

This Policy applies to business areas engaged in internal and external communications and employees who use social media in a professional or personal capacity. The Policy:

- defines social media and associated terms;
- details standards for professional and personal use of social media;
- provides information on the governance framework for establishing and managing a social media channel or tool including approval processes;
- provides information on how to comply with the Policy;
- provides information on inappropriate use of social media and risk management; and
- provides references for other relevant policies.

1. Scope

The term ‘social media’ refers to channels or tools that enable users to create and exchange content in a public digital space (see “Definitions” page 5).

This Policy applies to all IPC employees and third parties who use social media in a professional or personal capacity.

This Policy is informed by the NSW Department of Justice Social Media policy, which in turn is informed by Department, state, federal and international policies, guidelines and legislation including:

- NSW Government Social Media Policy and Guidelines
- *Government Information (Public Access) Act 2009* (NSW)
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *State Records Act 1998* (NSW)
- *Anti-Discrimination Act 1977* (NSW)
- Department’s Code of Conduct (see “Definitions” page 5)
- Information Technology Services (ITS) Information Security Policy
- Web Content Accessibility Guidelines 2.0
- Social Media Policy (August 2011) Corrective Services
- Official Use of Social Media, NSW Registry of Births, Deaths & Marriages
- Consumer, Trader and Tenancy Tribunal Social Media Policy (Consumer and Commercial Division of the NSW Civil and Administrative Tribunal)

It is also informed by the:

- IPC Business Plan
- IPC Code of Conduct
- IPC Privacy Management Plan

This Policy will apply from the date of effect.

2. Purpose

The purpose of this Policy is to support the IPC's participation in social media and employees' participation in social media on a professional and personal basis while adhering to the IPC Code of Conduct. (see "Definitions" page 5).

Corporate and personal risk is inherent in engagement of government employees in networked technologies which are: rapidly emerging and evolving; available around the clock; and used by a large number of employees in either a professional or personal capacity.

This Policy aims to limit the risk of damage to the IPC, its employees and clients, by establishing and making provision for the regular review of standards of use in relation to social media.

Aligned with the *NSW Government Social Media Policy and Guidelines*, as well as the NSW Department of Justice Social Media Policy, this Policy is intended to assist employees responsible for delivering IPC communications and engagement strategies which utilise social media, to consistently achieve the following:

- **Openness**: using social media to share and promote access to information and be transparent and accountable
- **Collaboration**: creating opportunities to listen to and engage with the public, employees, and industry in community building, policy discussion and service design
- **Responsiveness**: empowering employees to use social media to respond quickly to customer and emerging issues
- **Reliability**: supporting a consistent, quality experience
- **Appropriateness**: using social media in a manner that is consistent with public sector values, legal requirements, related policies, and codes of conduct.

This Policy does not mandate the use of social media. It provides a framework for best-practice in considering whether specific social media channels best meet business needs and assessing risks and benefits.

It is intended to be read in conjunction with IPC Social Media Procedures which defines the process for creating, administrating and monitoring any IPC presence on social media.

At the time of the release of this Policy, the IPC has established a social media presence on Twitter, LinkedIn and You Tube.

3. Definitions

Administrator is an IPC employee who manages the technical details of establishing the social media channel. This is the Manager, Communications and Corporate Affairs (Manager CCA) and by delegation to Communications and Promotions Officers (x2).

Authorised representative is an employee who has been delegated by the Manager CCA to interact on social media on behalf of the IPC.

Content includes text, audio, visual (for example, photographs), audio-visual (such as video), real-time audio-visual (such as tele-conferencing) and geo-spatial information.

Department means the Department of Justice.

IPC means Information and Privacy Commission NSW

IPC Code of Conduct refers to the Code of Conduct which establishes the standards of employee conduct required by the IPC and outlines the responsibilities of employees and managers to achieve a workplace where appropriate ethical standards are maintained.

All employees are required to comply with this Code and any breach of the Code may lead to remedial or disciplinary action.

IPC Media Protocol refers to established clear guidelines relating to responses to media requests for information, approval processes for media releases, media statements, letters to the editor, speeches, handling crises and emergency situations, advertising approval process.

IPC Privacy Management Plan explains how the IPC manages personal information in line with the *Privacy and Personal Information Protection Act 2002* (NSW) (PPIP Act), and health information under the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act).

IPC Social Media Procedures refers to the document which outlines the process of requesting, establishing, administrating and evaluating an approved social media channel.

Employee means employee of the IPC and persons engaged to provide services, information or advice. Employees include permanent, temporary, casual, trainee, SES officers, contractors, and any member of the public sector service as defined in Part 4 of the *Government Sector Employment Act 2013*.

Moderator is an IPC employee who monitors online communications. The moderator may also answer general questions about the channel and respond to complaints. A moderator is also an authorised representative.

Personal use of social media means **you are not identified** as an employee of IPC.

Public Consultation means a formal invitation for public comment on a specific matter, for example a piece of legislation or public policy.

Professional use of social media means **you are authorised** to comment as a representative of the IPC.

Sharing tools are tools such as 'add this' that allows users to share information through a social media channel such as Facebook or Twitter.

Social media refers to applications or tools that enable creation and exchange of user-generated content over the internet. Social media may include (and is not limited to):

- social networking sites e.g. Facebook, Myspace, LinkedIn, Bebo, Yammer,

Google+

- video and photo sharing websites e.g. Flikr, YouTube, Instagram
- blogs, including weblogs, corporate blogs and personal blogs
- blogs hosted by media outlets, for example, 'comments' or 'you say' feature on smh.com.au
- micro-blogging, for example Twitter
- wikis and online collaborations, for example Wikipedia
- forums, discussion boards and groups, for example Google groups, Whirlpool
- vod and podcasting

- online multiplayer gaming platforms, for example World of Warcraft
- instant messaging including SMS, 'What's App'
- geo-spatial tagging (Foursquare)
- online encyclopaedias such as Wikipedia
- any other channels or tools that allows for creation and exchange of user-generated content.

The content of the IPC social media site will be informed by corporate reports and the specific statutory responsibilities of the two Commissioners.

Note: Social media applications and tools are not supported by ITS. Internet access to social media channels requires an application to IT ServiceDesk with approval from the relevant manager.

Third parties are individuals or groups contracted to supply service to the IPC but are not directly employed by the IPC. These parties may include, but are not limited to contractors and consultants.

Web Content Accessibility Guidelines 2.0 (WCAG 2.0) is the document produced by the World Wide Web consortium that provides standards, guidelines and conformance advice on website accessibility.

4. Request for social media presence

When considering whether to use social media to meet business needs, it is essential communications planning include consideration of existing communications context, a risk analysis and identification of ongoing governance and resources. Privacy and Information Access specific content will be considered by the relevant Commissioner or their delegate.

All requests to establish a social media presence must be provided in the form of a project proposal prepared by Corporate Communications and Affairs (CCA) and submitted to the CEO.

If the request to establish a presence on social media is instigated by a business unit other than CCA, CCA can assist in developing the project proposal to determine whether social media is an appropriate communication tool for the identified need and is aligned with IPC priorities.

4.1 Responsibility for social media presence

The CCA team, under guidance from the Manager CCA is responsible for the entire process including developing the project proposal for submission to the relevant Commissioner for content purposes and to the CEO for finalisation.

Once approved, CCA is responsible for:

- Creation of the IPC account/profile on a social media channel
- Management of the IPC account/profile on a social media channel including monitoring, administration, content creation and ongoing management.

The IPC email address used for the creation of social media accounts will be the IPC personal email address of the Manager CCA. This allows the channel to be monitored on an ongoing basis.

Refer to IPC Social Media Procedures for more information on each of the above process stages.

5. Professional use of social media

Before engaging in social media as a representative of the IPC, employees must be authorised by the CEO and Manager CCA and the Privacy Commissioner when representing privacy.

Authorised representatives **must**:

- disclose themselves as an IPC employee and use only an approved official account or avatar
- adhere to the IPC Code of Conduct (see "Definitions" page 5) at all times
- disclose and comment only on information readily available to the public
- ensure that all content published is accurate and not misleading, and complies with relevant legislation and IPC policies
- adhere to the IPC Media Protocol ("Definitions" page 5) where applicable
- ensure they are not the first to make an announcement unless specifically authorised to do so
- comment only in the area or areas in which they have been authorised to comment
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws
- respect copyright laws and fair use of copyrighted material and attribute work to the original author/source
- sight the written consent form/s authorising the use of a photo and/or video prior to uploading and/or linking the photo and/or video on the social media channel
- advise the Manager CCA of any engagement online with an external client, former external client, or their family and friends where there may be a real, potential or perceived conflict of interest
- only use personal or health information of individuals for the purpose for which it was collected and in accordance with the IPC Privacy Policy and the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002.*

Authorised representatives **must not**:

- use IPC social media channels for personal use including use of IPC email addresses
- post or respond to content that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order or otherwise unlawful
- use abbreviations, jargon, colloquialisms, clichés or ambiguous, technical or abstract terms
- use language that is discriminatory, antagonistic, insensitive, inflammatory, condescending or offensive
- use or disclose any confidential, operationally sensitive or secure information without authorisation from the relevant commissioner and/or CEO.
- disclose official information (whether confidential or not) unless authorised to do so or unless the information is already in the public domain
- disclose the personal information of external clients, colleagues or others

- post images of external clients, colleagues or others without their written permission (IPC image release form)
- collect personal information of individuals or groups posting, following or in interacting on the social media channel
- 'follow', 'like', 'retweet' 'tag' or 'share' content when not authorised or approved to do so by the Manager CCA
- publish material that could lead to contempt of court, criminal penalty or civil liability
- make any comment or post any material that might otherwise cause damage to the IPC's reputation or bring it into disrepute
- make a comment or endorsement that could be perceived as criticising the decisions, policies or practices of the IPC, Department of Justice cluster, or the NSW Government
- advertise, use or disclose their personal IPC email address without authorisation from the Manager CCA
- imply IPC endorsement of personal views
- endorse products, causes or opinions
- commit the IPC to any action or initiative unless they have authority, or have been authorised, to do so by the Manager CCA in the first instance
- publish content related to children without authorisation and seeking permission from the Manager CCA
- use social media to establish or maintain engagement with external clients, former external clients, their families or friends who know their identity as an employee of the IPC, where there is a real, potential or perceived conflict of interest or risk of bringing the IPC or the employee into disrepute.

Refer to section 5 of IPC Code of Conduct for further guidance.

6. Use of IPC social media channels/accounts by third parties

This Policy and the Social Media Procedures apply to third parties (see "Definitions" page 5).

Third parties who are working with the IPC or who are associated with a program, project or activity of the IPC are bound by the relevant documents that govern their conduct when engaging in social media. These documents may include but are not limited to: the IPC Code of Conduct, this Policy, and handbooks for contractors.

7. Moderation

Where a social media channel is created, the CCA must ensure moderation rules are made clear and published on the social media channel. All public consultation (see "Definitions" page 5), where public comment is invited, should be conducted through the IPC website, and where appropriate via the whole-of-government 'Have Your Say' website.

Moderation activities will likely be management of unsolicited public responses to content published on the IPC's social media channels. It is a primary responsibility of the CCA to ensure publicly contributed comments are moderated to meet policy and legislative requirements, particularly in regard to discrimination and defamation.

Moderation also warrants review and necessary actions to address:

- offensive comments or responses
- where a person alleges that a comment is defamatory, discriminatory or offensive and requests its removal
- accidental or malicious publishing of operationally sensitive material.

Failure to remove an offensive comment may contravene discrimination legislation.

The risk management process (see "Managing Social Media Risk", page 11) must address the availability of staff and technical access to the application in relation to moderation. During longer periods, when moderation will be unavailable, for example, at times of extended public holidays, public contributions must be temporarily suspended.

The risk management process must also address the risk of accidental or malicious publishing of operationally sensitive material such as (but not limited to) announcements that are still pending review and are not publicly available otherwise.

A standard IPC disclaimer (refer to appendix b in *IPC Social Media Procedures* should be posted on all social media channels that invite public comment and/or user-generated content.

7.1 Managing inappropriate disclosures

Adequate employee training, governance and resources for maintenance of the channel/s to appropriate standards as outlined in this Policy is required.

In the event of accidental or intentional publishing of content in breach of this Policy or the IPC Code of Conduct, including content of a sensitive, confidential or operational nature the content should be removed immediately; a record kept of the disclosure and other relevant information about circumstances and subsequent actions, taken in accordance with relevant IPC policy and statutory obligations.

Advice must be given as soon as possible to the Manager, CCA and Director Business Improvement.

Refer to section 5 of IPC Code of Conduct and IPC Privacy Management Plan for further guidance.

8. Meeting accessibility compliance

Social media channels must adhere to the WCAG 2.0 standards. Each social media tool has specific accessibility issues and, in turn, there are specific techniques which can be used to overcome them.

Refer to Media Access Australia's online report: *Sociability: social media for people with a disability*. This information is also included as Appendix G in the Department of Justice's *Social Media Procedures* document.

9. Breaches and disciplinary process

Breaches of policy are investigated and managed in accordance with sections 38-41 and 69 and 70 of the *Government Sector Employment Act 2013*. Further guidance is available on the Public Service Commission employment portal.

10. Identifying inappropriate use

Any employee seeing inappropriate or unlawful content, or content that may otherwise have been published in breach of this Policy, on IPC social media channels or tools, must report the circumstances to the Manager CCA.

Subject to the nature of the inappropriate use, issues will be addressed in conjunction with the relevant IPC Senior Executives.

11. Using photos and video

Approval must be given by the Manager CCA to publish a photo/s and/or video/s on a social media channel. Prior to publishing a photo/s and/or videos on a social media channel, permission must be sought from individuals appearing in the photo/s and/or video/s to use their image for online purposes (use IPC image release form).

12. Managing social media risk

The rapidly changing online environment means that risk management processes must be frequently reviewed for existing social media tools. The CCA team will conduct a risk assessment as part of the project proposal for new social media tools.

To protect reputation, information and intellectual property, and mitigate legal action, the IPC and its business areas must manage risks associated with using social media channels.

Effective social media risk management will address the four main risks produced by social media. They are:

1. damage to reputation that can result in a loss of trust or credibility
    - to the IPC
    - to colleagues
    - to an individual employee
2. release of sensitive or confidential information, whether accidental or malicious
3. engagement in social media, while not violating laws and regulations, which causes a personal or professional disadvantage or causes damage to the IPC's reputation or brings it into disrepute
4. appropriation of the IPC's social media platform including establishment of fake pages that provide false information or otherwise acting maliciously.

To ensure relevant aspects of business operations and the external environment are understood, stakeholders and staff must be involved in the risk management process.

A risk management plan must be developed for inclusion in the project proposal requesting a social media channel. Staff involved in managing social media channels must be familiar with the administration of risk management activities.

13. Recordkeeping

As content begins to be created or received by means of social media channels, the CCA must develop channel-specific strategies to ensure content generated by the channel is maintained and can be accessed as required.

The recordkeeping strategy is determined by what content is being generated by the social media channel:

- the risk and long-term value of the content
- the application to be used to capture and maintain content
- how long the records need to be kept.

The strategy that is implemented will be dependent upon which best meets the needs and technological environment while making an assessment of the potential risks involved.

Detailed information relating to recordkeeping as it relates to social media communications and the *State Records Act 1998* can be found online at: http://www.records.nsw.gov.au/recordkeeping/advice/designing-implementing-and-managing-systems/strategies-for-managing-social-media-information/strategies-for-managing-social-media-information

14. Personal use of social media

The IPC recognises employees may use social media in their personal life. This Policy does not intend to discourage nor unduly limit personal expression online or use of social media channels.

As an employee of the IPC and the NSW Government, there is, however, a risk of damage including legal and reputational (directly or indirectly and accidentally as well as with intention) to those entities via personal use of social media as well as to the individual employee.

Employees must adhere to the IPC's Code of Conduct and to this Policy in their use of social media in a personal capacity.

Refer to section 5 of IPC Code of Conduct for further guidance.

14.1 Reasonable and unreasonable personal use

Employees required to have internet access to perform tasks as outlined in their role responsibilities or using their own mobile devices, when accessing social media in the workplace in either a personal capacity or for professional uses, must do so in accordance with the this Policy, ITS Policies and Procedures and the IPC's Code of Conduct.

15. Related policies and procedures

- IPC Business Plan
- IPC Code of Conduct
- IPC Media Protocol
- IPC Privacy Management Plan
- IPC Social Media Procedures
- ITS Information Security Policy
- ITS Information Security Policy 7.2 Acceptable use of Assets

16. References

- ***NSW Department of Justice Social Media Policy*** **which references:**

- NSW Government Social Media Policy and Guidelines
- Personnel Handbook
- NSW 2021 NSW Government ICT Strategy 2012
- M2012-10 Open Government
- M2009-11 NSW Standard on Digital Recordkeeping
- *Government Information (Public Access) Act 2009*
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Public Sector Employment and Management Act 2002*
- *State Records Act 1998*
- *Anti-Discrimination Act 1977 (NSW)*
- *Coroners Act 2009 (NSW)*
- Department of Education and Training NSW, *Social Media Policy*
- Department of Education and Training NSW, *Social Media Guidelines*
- Department of Justice Victoria, *Social Media Policy*
- Family and Community Services NSW, *Social Media Policy*
- Code of Conduct (2009) Attorney General's Division
- Guide to Conduct and Ethics (2010) Corrective Services
- Code of Conduct (July 2010) Juvenile Justice
- Juvenile Justice Dignity and Respect Policy
- Dignity and Respect Policy (former Attorney General's Division)
- CSNSW Media Policy
- Department of Justice Media Policy
- Social Media Policy (August 2011) Corrective Services
- Official Use of Social Media, NSW Registry of Births, Deaths and Marriages
- CTTT Social Media Policy and Guidelines
- Department IT Policies and Procedures
- *Future Proof – Protecting our digital future*, State Records NSW
- (http://futureproof.records.nsw.gov.au/)
- *Guideline 20 – Keeping web records*, State Records NSW
- *Guidelines 24 - Record management and web 2.0*, State Records NSW
- *Managing complaints and other feedback policy*, Community Relations Unit
- Department of Justice Accessibility for Web Communications Policy

17. Document information

Title:	IPC Social Media Policy
Business Unit:	Information and Privacy Commission
Author:	Communications and Promotions Officer
Owner:	
Approver:	CEO, Information Commissioner
Date of Effect:	
Next Review Date:	
File Reference:	
Key Words:	Social Media

18. Document history

Version	Date	Reason for Amendment
1.0	November 2014	Initial Draft
1.1	December 2014	A/Director Investigation and Review comments
1.2	December 2014	NSW Privacy Commissioner comments
1.3	January 2015	Information Commissioner and CEO comments
1.4	March 2015	Update date of effect following approval (from Dec 14 to Mar 15)