Social Media Policy

The Department recognises the opportunity social media provides for people to gather in online communities of shared interests to create, share and consume content as well as its potential for use in engagement with the Department's internal and external stakeholders and clients.

The intention of this policy is to establish a culture of openness, trust and integrity in activities around social media. It provides a governance framework for managing social media channels and tools on behalf of the Department and provides employees with standards of use as they engage in social media on a professional and personal basis in order to limit risk to the Department, its clients and employees.

This policy complements the NSW Government Social Media Guidelines and its directive on Open Government *(M2012-10 Open Government)*. While the Policy encourages consideration of use of social media it does not mandate adoption of social media by all business areas; it rather makes the use of social media an option to fulfil business needs where appropriate and also encourages them to give careful consideration to its benefits and risks. It provides a framework, guidelines and standards within which the Department's business areas can develop channels when appropriate to serving identified, citizen-centric needs.

All employees are responsible for knowing and understanding this Policy. Business areas must make reference to this Policy when documenting their own business rules in regard to the use of social media. This Policy will supersede all area or agency-based social media policies.

The Social Media Procedure document provides instructional information about requesting, gaining approval for, establishing and managing a social media channel.

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 Departmental 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.

Table of Contents

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 3. Definitions)

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

This Policy 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)
- *State Records Act 1998* (NSW)
- *Anti-Discrimination Act 1977* (NSW)
- Department's Code of Conduct (see 3. Definitions)
- 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
- Health Records and Information Privacy Act 2002
- Consumer, Trader and Tenancy Tribunal Social Media Policy (Consumer and Commercial Division of the NSW Civil and Administrative Tribunal)

This Policy supersedes all area or agency-based policies on social media. It is to be read in conjunction with the Social Media Procedures document.

Business area managers must be aware of their responsibilities under this Policy and align procedural documents related to social media to the Social Media Policy and Social Media Procedures documents.

This Policy will apply from the date of effect.

2. Purpose

The purpose of this Policy is to support business areas' participation in social media and employees' participation in social media on a professional and personal basis while adhering to the Department's Code of Conduct. (see 3. Definitions)

Corporate and personal risk is inherent in engagement of government employees in networked technologies which are: rapidly emerging and evolving; available at all times and used by almost all in a professional or personal capacity. By defining standards of use and keeping standards under regular review, the Policy seeks to limit, as far as possible, the risk of damage to the Department, its clients and employees.

Aligned with the *NSW Government Social Media Policy and Guidelines*, this Policy is intended to assist employees and the Department in successful engagement through social media and 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 employees, the public 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.

While the Policy encourages consideration of use of social media it does not mandate adoption of social media by all business areas; it rather makes the use of social media an option to fulfil business needs where appropriate and also encourages them to give careful consideration to its benefits and risks. It provides a framework, guidelines and standards within which the Department's business areas can develop channels when appropriate to serving identified, citizen-centric needs.

3. Definitions

Administrator is a Department employee who manages the technical details of establishing the social media channel. The Communications Unit and Information Technology Services (ITS), Information Security appoints administrators. Administrators are able to act as authorised representatives and as moderators with approval from local business areas.

Authorised representative is an employee who has been approved, by their relevant head of division or agency, to interact on social media on behalf of the Department in that division or agency's social media. Social Media Procedure 6.1 details the approval process for staff undertaking this role.

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 Police and Justice.

Department's Code of Conduct refers to an employee's relevant existing Code of Conduct and includes the Corrective Services Division Code of Conduct, the Juvenile Justice Division's Code of Conduct, and the Code of Conduct applying to all other Divisions. A code of conduct is a guide to ethical workplace behavior, setting out the minimum standards expected of employees of the Department. It applies to all aspects of employment, including the workplace environment and workplace activities, and provides an ethical framework for decisions, actions and behaviour.

Department's Media Policy refers to an employee's relevant existing Media Policy and includes the Corrective Services Division Media Policy, the Juvenile Justice Media Policy, and the Media Policy applying to all other Divisions.

Employee means employee of the Department and persons engaged to provide the Department with services, information or advice. Employees include permanent, temporary, causal, trainee, ministerial staff, SES officers, contractors, non-judicial statutory appointments and any member of the public sector service as defined in Part 4 of the *Government Sector Employment Act 2013*.

Moderator is a Department 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 a Department employee.

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 Department representative.

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 third party 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 eg Facebook, Myspace, LinkedIn, Bebo, Yammer, Google+
- video and photo sharing websites eg 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.

Note: Social media applications and tools are not supported by ITS, nor does the Department advocate for, support or recommend any individual social media channel or tool. Internet access to social media channels and tools is managed by the ITS security team and must be used in accordance with the Department's ITS Information Security Policy 7.2 Acceptable Use of Assets.

Third parties are individuals or groups not directly employed by the Department and contracted to supply services to the Department. Third parties are also individuals or groups required by the justice system in delivering services and functions overseen by the Department. These parties may include, but are not limited to: Jurors, Guardians ad Litem, Justices of the Peace, 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.

A request for a social media presence must be provided in the form of a business case to the Communications Unit. The Unit will assess the case according to how well the proposed social media addresses an identified communication need and how it aligns with Department priorities. The Unit may assist a business area client to develop their proposal.

All requests to use social media must be approved by the Director, Strategic Communications who assesses the request within the context of existing Department-wide plans, strategies and goals.

At the time of the release of this Policy, the Department has established a social media presence on You Tube.

5. Professional use of social media

Professional use of social media includes engagement in managing and responding to public contributions on a Departmental social media channel. (For personal use of social media see Section 14.)

Before engaging in social media as a representative of the Department, employees must be authorised by the relevant head of Division or Office. (See Social Media Procedures 6.2 for the authorisation process).

Authorised representatives **must**:

- disclose themselves as an employee of the Department and use only an approved official account or avatar
- adhere to the Department's Code of Conduct (see 3. Definitions) at all times
- disclose and comment only on information classified as information in the public domain
- ensure that all content published is accurate and not misleading and complies with relevant legislation and Department policies
- adhere to the Department Media Policy (see 3. Definitions)

- ensure they are not the first to make a Department 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
- disclose to their business area manager 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
- must only use personal or health information of individuals for the purpose for which it was collected and in accordance with the Department's privacy policies and the *Privacy and Personal Information Protection Act* and the *Health Records and Information Privacy Act*.

Authorised representatives **must not**:

- use Department social media channels for personal use including use of Departmental email addresses (see *Information Security Policy 7.2 Acceptable Use of Assets)*
- 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 their business area manager, including but not limited to: rosters, procedures, unpublished judgements and suppressed information

- 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 (see the Social Media Procedures document for a copy of the Department Written Consent 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 their business area manager
- 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 Department'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 Department or the NSW Government
- advertise, use or disclose their personal Department email address without authorisation from their business area manager
- imply Department endorsement of personal views
- endorse products, causes or opinions
- commit the Department to any action or initiative unless they have authority, or have been authorised, to do so by their business area manager
- publish content related to children without authorisation and seeking permission from the business area manager, Children represent a part of the Department's audience. There are particular restrictions on the publication of material relating to children. The publication of the identity of a child involved in Children's Court proceedings is prohibited and is an offence[1]. Publication of Department material identifying children should be considered carefully and advice sought if necessary.

[1] See section 105 of the *Children and Young Persons (Care and Protection) Act 1998.*

- 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 Department, where there is a real, potential or perceived conflict of interest or risk of bringing the Department or the employee into disrepute.

5.1 Employees representing a Union

Comments made on matters relating to union business by members of unions in their capacity as a local delegate within the Department or by union office holders employed by the Department are permitted, as long as the individual makes clear that the comments are about matters that are only related to union business and are made in a union capacity and not as a staff member or on behalf of the Department.

An employee representing a union must adhere to the Department's Code of Conduct.

6. Use of social media by third parties

This Policy and the Social Media Procedures apply to third parties (*see 3 Definitions*).

Third parties who are working with the Department or who are associated with a program, project or activity of the Department or are participating in the justice system 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 Court Security Regulation 2011, the Court Security Act 2005, the Department's Code of Conduct, handbooks for contractors and Jury Directions.

It is the responsibility of the business area manager, when engaging third parties, to ensure that the relevant document/s that govern the conduct of the third party or parties complies with the professional and personal use of social media standards outlined in this policy.

7. Moderation

Where a social media channel is created, the business area must ensure moderation rules are made clear and published on the social media channel[2]. All public consultation (See 3. Definitions), where public comment is invited, should be conducted through the whole-of-government 'Have Your Say' website.

Moderation activities in the Department will likely be management of unsolicited public responses to content published on the Department's social media channels. It is a primary responsibility of the relevant business area manager 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. Business area managers must ensure that appropriate actions are taken on availability of staff and technical access to the application. During longer periods, when moderation will be unavailable, for example, at times of extended public holidays, public contributions must be temporarily suspended.

Business area managers owning the social media channel must outline procedures to manage the risk of accidental or malicious publishing of operationally sensitive material such as (but not limited to) proceedings of court, announcements that are still pending review and is not publicly available otherwise (see 7.1).

The standard Department disclaimer (See Appendix H in the Social Media Procedures document) is to be used for all social media channels that enable public users to make comments.

See the Social Media Procedures, Appendix E, for an example of moderation guidelines.

7. 1 Managing inappropriate disclosures

Business areas engaged in social media are required to have adequate employee training, governance and resources for maintenance of their channel/s to appropriate standards as outlined in this Policy. In the event of accidental or

[2] The NSW State government has launched a community consultation website haveyoursay.nsw.gov.au. It is mandatory for all government departments to use this site for seeking and collecting comments from the public.

intentional publishing of content in breach of this Policy or the Department's 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. Advice must be given as soon as possible to the business area manager and the Communications Unit. Ongoing responses may include an analysis of the reasons for the event and formulation of responses that would mitigate future similar risks.

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. See *How to meet accessibility standards* in Appendix G of the Social Media Procedure document for more information.

As a matter of equity of access, business areas must not rely on social media as the main or only source for publishing content and must consider complementary channels for publishing information.

9. Non-compliance

Depending on the circumstances, non-compliance with this policy may constitute a breach of employment or contractual obligations, misconduct (under the Department's *Code of Conduct – See3. Definitions*), sexual harassment, discrimination, or some other contravention of the law. *Those who fail to comply with this policy may face disciplinary action and, in serious cases, termination of their employment or engagement.*

Employees engaged in professional and personal use of social media must adhere to the Department's Code of Conduct.

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 Department social media channels or tools, must report the circumstances to the relevant business area manager or the Communications Unit communications@justice.nsw.gov.au.

Subject to the nature of the inappropriate use, issues will be addressed in conjunction with the relevant Senior Executives of the Department who may include the Secretary, Executive Director Human Resources, Executive Director Information Technology Services, and Director Strategic Communications.

11. Using photos and videos

Approval must be given by the business area manager 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. A copy of the Department Written Consent Form (see Appendix F) can be found in the Social Media Procedures document.

Note: all videos must be published to the Department's You Tube channel – JusticeNSW (http://www.youtube.com/user/JusticeNSW). See Social Media Procedures Appendix I for a template form to request upload and publishing of videos on the JusticeNSW You Tube channel.

12. Managing social media risk

To protect reputation, information and intellectual property, and mitigate legal action, the Department 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 Department
    - 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 Department's reputation or brings it into disrepute

4. appropriation of the Department or business area 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.

The Department has risk management policies, guidelines and training that support risk management activities. In requesting a social media channel, the business area must submit a risk management plan as part of their social media brief. Staff involved in managing social media channels must be familiar with the administration of risk management activities.

13. Record keeping

As content begins to be created or received by means of social media channels, the Department and its business areas using a social media channel must develop strategies to ensure content generated by the channel is maintained and can be accessed as required.

The record-keeping 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 of the Department and business area while making an assessment of the potential risks involved.

Detailed information about social media record keeping can be found online at State Records NSW, *Future Proof – Protecting our digital future*.

14. Personal use of social media

The Department 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 Department 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 Department's Code of Conduct and to this Policy in their use of social media in a personal capacity.

Employees **must not**:

- imply they are authorised to speak as a representative of the Department or the NSW Government, nor give the impression that their views express those of the Department or the NSW Government
- disclose Department email addresses or use any Department logos or insignia
- use the Department email system for any personal postings or interactions over social media platforms
- publish content that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, breaches an individual's privacy, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful
- publish content (see 3. Definitions) or information acquired in the workplace or while on duty including and especially relating to colleagues and clients
- use social media in the workplace in a way that allows identification of their location where this creates risk for the individual or the Department
- bully and/or harass colleagues. Workplace bullying and harassment may include any comments employees make online in their own private social networks or out of office hours. Abusive, harassing, threatening or defaming posts are a breach of the Department's Code of Conduct.
- 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 Department, where there is a real, potential or perceived conflict of interest or risk of bringing the Department or the employee into disrepute.

14. 1 Reasonable/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 Department's Code of Conduct.

Department resources must not be used to access or post any material that is fraudulent, harassing, threatening, bullying, embarrassing, sexually explicit, profane, obscene, racist, sexist, intimidating, defamatory or otherwise inappropriate or unlawful.

Employees must not use the Department's internet and computer resources to provide comments to journalists, politicians and lobby groups other than in the course of their official duties

Use of personal devices to access social media must adhere to ITS Policies and Procedures (see *Information Security Policy 7.2 Acceptable Use of Assets)* and the Department's Code of Conduct.

15. Related policies and procedures

- NSW Government Social Media Policy and Guidelines
- ITS Information Security Policy
- ITS Information Security Policy 7.2 Acceptable use of Assets
- Social Media Procedures

16. 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

Health Records and Information Privacy Act 2002

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 & 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

DAGJ Media Policy

Social Media Policy (August 2011) Corrective Services

Official Use of Social Media, NSW Registry of Births, Deaths & 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

DAGJ Accessibility for Web Communications Policy

17. Document information

Status:	Version 1.0 Final - Current
Title:	Social Media Policy
Business Area:	Communications Unit, DAGJ
Author:	Communications Unit, DAGJ
Approver:	Secretary
Date of Effect:	2nd April 2014
Next Review Date:	One year from effect
File Reference:	
Key Words:	Social media, communications, digital communications, internet

18. Document history

Version	Date	Reason for Amendment
0.1	07/09/2012	Released to Juvenile Justice, Corrective Services, Information Technology Services, Justice Legal Services, Victims Services,
0.2	03/02/2013	Incorporated comments from previous round of review. Released for another round of feedback from the above groups and Courts & Tribunal Services, Trustee and Guardian, BDM.
0.3	03/02/2014	Incorporated feedback from the above round of review and Submitted to Executive
0.4	07/03/2014	Feedback incorporated from: Courts and Tribunals Human Resources Trustee and Guardian Juvenile Justice Division Corrective Services Division
1.0	20/03/2014	Submitted for final endorsement