information and privacy commission
new south wales

IPC Social Media Policy

Updated June 2021

Purpose

1. The purpose of this policy is to support IPC's participation in social media and employees' participation in social media on a professional and personal basis while adhering to the Information and Privacy Commission's (IPC) Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees.
2. IPC, as the NSW statutory authority for information access and privacy regulation, must be, and must be seen by the public to be, an independent authority that upholds the objects of the legislation that it administers. As part of its function, IPC promotes and protects privacy and information access rights in NSW. It is therefore of upmost importance that postings on social media platforms which are seen to represent the IPC do not impinge on those rights or bring the IPC's reputation as an independent regulator into disrepute.

Policy Statement

3. The IPC 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 IPC's internal and external stakeholders.
4. 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 IPC and provides employees with standards for acceptable use as they engage in social media on a professional and personal basis in order to limit risk to the IPC, its stakeholders and employees.
5. This policy complements the NSW Department of Customer Service's Social Media Policy, NSW Government Social Media Guidelines, Digital Government Strategy and NSW Government Open Data Policy directives. While the Policy encourages consideration of use of social media, it does not mandate adoption of social media by the IPC; it rather makes the use of social media an option to fulfil business needs where appropriate and encourages the IPC to give careful consideration to its benefits and risks. It provides a framework, guidelines and standards within which the IPC can develop channels when appropriate to serve identified, citizen-centric needs.
6. All employees are responsible for knowing and understanding this policy. This policy will replace any previous social media policies.

Scope

7. This policy applies to all employees of the IPC, third parties contracted to provide services to or on behalf of the IPC, and IPC stakeholders who use social media in a professional or personal capacity.
    - **Professional use, sections 9 to 65** – Personnel representing the IPC and managing social media channels on behalf of the IPC.
    - **Personal use, sections 66 to 96** – Personnel who do not disclose that they work for the IPC.
    - IPC Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees**, section 93.**

Communication

8. This policy will be communicated to all staff via the CEO's communications and education sessions delivered by the Manager, Communications and Corporate Affairs. This policy and related documents will be placed in EDRMS and published on the IPC website as part of the IPC's open access program.

Implementation

9. The IPC runs social media assets under a central governance model to build holistic brand awareness, improve efficiency and to mitigate risk.
10. Social media assists the IPC in delivering on recommendations outlined in the *2017 NSW Digital Government Strategy* to improve stakeholder 'user experience' both internally and externally.
11. Social media assists the IPC in delivering on and evaluating against State, Premier and IPC priorities and objectives.
12. When considering whether to use social media to meet business needs, it is essential to conduct an audit of current communications and identify why a social media presence is required. This includes defining objectives, determining target audiences, providing risk analysis and identification of ongoing governance and resources.
13. A request for the establishment of a new form of social media presence must be provided in the form of a business case or briefing note to the Director, Business Improvement. The Director will assess the case according to how well the proposed social media channel addresses an identified communication need and how it aligns with the IPC's priorities. The Manager, Communications and Corporate Affairs may assist a business area to develop their proposal.
14. All requests to use social media must be approved by the Director, Business Improvement who assesses the request within the context of existing IPC's plans, strategies and goals.
15. All social media accounts will have a yearly review providing recommendations on issues management, improvements to strategy and content, and necessity.

Copyright and Intellectual Property

16. The IPC must ensure that any materials published on official social media pages that are not the property of the IPC or another NSW government agency do not infringe any third-party intellectual property rights including copyright in relation to text, images or videos and trademarks.
17. There may be licensing or copyright issues that either prevent the publishing of external copyrighted material onto social media or require payment of a licence fee or royalties to do so. If in doubt, seek legal advice from Legal Counsel and Regulatory Advice (LCRA).

Professional Profiles

18. Staff authorised by their business area manager to administer a social media account on behalf of the IPC must create an official social media profile using an approved work email address and avatar. All staff profiles created using work emails must be registered with the Manager, Communications and Corporate Affairs for inclusion in the Communications and Corporate Affairs Handbook.
19. Official social media profiles remain the property of the IPC and must only be used for the official reason the profile was created for. Professional work profiles are subject to audit and may be deleted if the profile or its use contravenes the IPC's policies.

Passwords

20. For more information about passwords and information technology security, please read the DCS information security page.

Professional Use of Social Media

21. Professional use of social media includes managing and responding to public contributions on the IPC's social media channels.
22. Before engaging in social media as a representative of the IPC, employees must be authorised by a member of the Executive
23. If advice is required, regarding social media content please contact the Manager, Communications and Corporate Affairs.
24. Authorised representatives must:
    - adhere to the IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees (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 factually accurate and not misleading and complies with relevant legislation and IPC policies
    - adhere to the IPC's Media Protocol
    - ensure they do not make an IPC 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,
    - 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 IPC's privacy policies and the *Privacy and Personal Information Protection Act* and the *Health Records and Information Privacy Act*.
25. Authorised representatives must not:
    - use IPC social media channels for personal use including use of an IPC issued email address
    - 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 language that is discriminatory, defamatory, 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; procedures, reviews and casework, matters before NSW Civil and Administrative Tribunal (NCAT), and publications currently under review
- 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 interacting on the social media channel
- post or comment on non-IPC social media platforms, including forums and blogs attempting to influence commentary or change opinions
- '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 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 or the NSW Government
- advertise, use or disclose their personal IPC email address without authorisation from their business area manager
- imply the IPC's 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 their manager
- publish content about children or protected persons in violation of particular restrictions on publication, or publishing content without authorisation. Advice should be sought when considering publication of material identifying children
- use social media to establish or maintain engagement with applicants or clients, former external clients or applicants, 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.

Paid Posts and 'Boosts'

26. Paid posts, referred to as 'boosts' are paid social media content that are informed by the *Government Advertising Act 2011* (NSW). Paid posts are considered advertising. Under the NSW Government Advertising Guidelines, campaigns are required to be presented objectively, in a fair and accessible manner. Government advertising campaigns may only be used to achieve the following objectives:

    - encouraging changed behaviours or attitudes that will lead to improved public health and safety or quality or life;

- maximising public and commercial compliance with laws and regulations;
- encouraging use of government products and services;
- encouraging public involvement in government decision-making;
- raising awareness of a planned or impending initiative and reporting on performance in relation to NSW Government undertakings;
- assisting in the preservation of order in the event of a crisis or emergency; and
- recruiting staff, disseminating important statutory information and promoting business opportunities with the NSW Government.

27. Paid social media posts must not mention or include images of Ministers, unless approved.
28. Paid social media posts will be determined in consultation between the relevant business area, the Manager, Communications and Corporate Affairs and the Director, Business Improvement.

Use of Social Media by Third Parties

29. 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 the conduct of staff of the IPC when engaging in social media. These documents will include the IPC's Code and Conduct.
30. It is the responsibility of the manager or director, 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.

Paid Influencers

31. The IPC policy on paid influencers is that they are not to be engaged. As independent entities, their online conduct be it past, present or future, requires management by IPC staff beyond the scope or capacity of their workday duties. This creates a reputational risk for the IPC that contravenes best practice.

Moderation and Risk Management

32. 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.
33. Effective social media risk management will address the four main risks produced by social media. They are:

I. damage to reputation that can result in a loss of trust or credibility
   - to the agency (IPC)
   - to staff
   - to an individual employee

II. release of sensitive or confidential information, whether accidental or malicious

III. 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.

IV. appropriation of the IPC's social media platform including establishment of fake pages that provide false information or otherwise acting maliciously.

34. Business area managers owning the social media channel must outline procedures to manage the risk of accidental or malicious publishing of operationally sensitive material. (See, Professional Use of Social Media, paragraph 21).
35. The Communications & Corporate Affairs unit must ensure moderation rules, known as Terms of Use, are accessible and published on the social media channel or made available on the IPC website. See paragraph 56.
36. Monitoring and evaluating online comments are an integral part of social media engagement. Online comments by NSW citizens are a valuable resource providing public insight and sentiment. This is distinct to official public consultation (See Definitions), where public comment is invited. Official consultation is to be conducted through the whole-of-government 'Have Your Say' website or IPC 'Have Your Say' website for IPC-specific consultations.

Responding to Comments

37. Social media comments come in a variety of forms such as opinions, rhetorical statements, or direct questions and are an integral part of online discussion and public debate. Not all comments that appear on IPC social media accounts are directed at or require a response from the moderator. When a comment does require the moderator to respond, approved responses need to be sourced from official Fact Sheets or requested from subject matter experts in the business area that owns the source material.
38. Business area managers must outline procedures to manage responses to online comments. This includes closely liaising with the Communications and Corporate Affairs team, subject matter experts and relevant senior management to formalise approved responses.
39. For further information on standards for managing complaints and feedback about the IPC please see the IPC Unreasonable Client Conduct Policy.

Managing Risk

40. The IPC 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 business case. Staff involved in managing social media channels must be familiar with the administration of risk management activities.
41. It is a primary responsibility of the directors to ensure publicly contributed comments are moderated to meet policy and legislative requirements particularly regarding discrimination and defamation.
42. 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.
43. Failure to remove an offensive comment may contravene discrimination legislation. Business area managers must ensure that appropriate resources are allocated to social media monitors, including technical support, software upgrades and staff training.
44. See the IPC's Media Procedures, for an example of moderation guidelines.

Managing Inappropriate or Unlawful Disclosures

45. Staff managing 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. Inappropriate or even unlawful disclosures of information may occur intentionally but may also be a result of an accidental disclosure. Where inappropriate publishing of content, including content of a sensitive, confidential or operational nature occurs in breach of this policy, the IPC's Code of Conduct, and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees, the content should be removed immediately; and a record kept of the disclosure and other relevant information about circumstances and subsequent actions. Please see the IPC voluntary data breach notification page for more information.
46. Advice must be given as soon as possible to the Director Business Improvement and the Manager, Communications and Corporate Affairs. Ongoing responses may include an analysis of the reasons for the event and formulation of responses that would mitigate future similar risks. All staff should be familiar with the IPC's Privacy Management Plan.
47. **All unlawful disclosures of personal or health information are governed by** the *Privacy Personal Information Protection Act 1998* (PPIP Act) and *Health Records Information Privacy Act 2002* (HRIP Act). To seek advice and report any breaches or potential breaches of privacy please contact your Manager.

Identifying Inappropriate Use

48. 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 relevant business area manager and the Manager, Communications and Corporate Affairs via communications@ipc.nsw.gov.au.
49. Alleged inappropriate use will be investigated under the IPC code of conduct policy

Self-reporting Online

50. Members of the public will from time to time, post information about an alleged crime, or emergency/information access and/or privacy breach (personal or otherwise).
51. When this occurs, it is important to capture the information (screen grab) for future reference and/or use for evidentiary/intelligence purposes and archive.
52. Encourage the author to contact police or the appropriate agency directly with any further information.
    - Emergencies: for any member of the public stating they intend to cause self-harm or harm to others, please tell them to call 000 (24 hours).
    - Non-emergency: for any member of the public who wants to leave feedback on IPC services and programs direct them to IPC's general enquiry inbox at ipcinfo@ipc.nsw.gov.au
    - Reporting a crime: call 1800 333 000 or https://nsw.crimestoppers.com.au/
53. For any member of the public in a non-emergency situation who wishes to speak to a counsellor, please advise them to call Lifeline on 13 11 14
54. For any member of the public in a non-emergency situation who needs advice on mental health pathways, please advise them to call the Mental Health Line 1800 011 511.
55. If a citizen has posted content deemed sensitive and/or inappropriate, the administrator should hide the information from public view, or capture the information and delete it from the page, if hiding the information from public view is not possible.

56. For further information on standards for managing complaints and feedback about the IPC please see the IPC Unreasonable Client Conduct Policy.

Template "Terms of use" for External Audiences

57. When using the IPC's social media platforms, you agree to comply with our terms of use as outlined below:

I. We welcome your comments on the IPC's social media, and ask that you show courtesy, respect and do not use the platforms to abuse, defame, provide offensive or inappropriate content for unlawful purposes.

II. To preserve the integrity of the IPC's decision making, comments will not be provided on any aspects of pending, current or finalised matters before NCAT.

III. Information posted on our sites is not intended to be legal advice and should not be used as such.

IV. The IPC asks that you protect your own personal privacy and that of others by not including personal information of yourself or of others to the page (for example, names, email addresses, private addresses or phone numbers).

V. Opinions or views expressed on the IPC's social media sites by people external to the IPC represent the thoughts of individual bloggers and online communities, and not the IPC.

VI. While the IPC makes reasonable efforts to monitor and/or moderate content posted on its social media platforms, we cannot always respond in real-time. The IPC's social media platforms are monitored during business hours and responses to comments will only be provided during business hours (excluding public holidays).

VII. The IPC reserves the sole right to review, hide or delete any comments it deems inappropriate. Comments including, but not limited to, the following may be deleted or hidden:

- abusive or hurtful comments about a blogger, an individual, another participant or IPC employees, which may include:
    - inappropriate or discriminatory language (e.g. profanity, racial, ethnic, disability, age, religion or gender-based)
    - personal attacks or defamatory statements or comments (e.g. negative personal or untrue comments about a person)
- views that impersonate or falsely represent any other person or falsely state or misrepresent affiliation with a person or entity;
- irrelevant and redundant comments to the topic being discussed (e.g. promotion of events, groups, websites, organisations and programs not related to or affiliated with the IPC)
- comments that violate the privacy of IPC staff, members, clients or stakeholders
- details relating to lodging complaints, seeking legal advice or discussing any matters brought to the IPC that are pending, current or finalised
- content that may or would constitute a criminal offence or give rise to civil liability, or that otherwise violates any local, provincial, national or international law or regulation in the world (or encourage others to do so).

VIII. Persistent inappropriate use of the IPC's social media platforms will lead to the user being blocked from the IPC's platforms, and/or reported to the platforms Administrator for breach of their terms of use.

IX. Links from the IPC's social media sites to other websites are provided as a guide only and do not constitute endorsement of those sites by the IPC and as such we are not responsible for the content of external websites.

X. By submitting content to the IPC's social media platforms, you understand and acknowledge that this information is available to the public and is considered a public record.

XI. The IPC makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the contents on its social media platforms and expressly disclaims liability for errors and omissions in their content. No warranty of any kind, implied, expressed, or statutory, including, but not limited to, the warranties of non-infringement of third-party rights, is given with respect to the contents of social media or its links to other online resources.

Compliance and image permissions

Using photos and videos

58. Approval must be given by the business area manager to publish a photo/s and/or video/s on a social media channel.

59. 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 consent form is available in EDRMS (D20/009282/DJ).

60. *Note: all videos must be published to the department's You Tube channel – IPCNSW (http://www.youtube.com/user/IPCNSW).*

Meeting accessibility compliance

61. Social media channels must adhere to the Web Content Accessibility Guidelines (WCAG) 2.0 and 2.1 standards.

62. 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.

Record keeping

63. As content begins to be created or received by means of social media channels, the IPC will ensure that content generated by the channel is maintained and can be accessed as required.

64. In some cases, social media interactions may be evidence for legal or investigation purposes. Staff should implement a strategy for social media records management that is in line with IPC Social Media Procedures, IPC's Functional Retention and Disposal Authority and the *State Records Act 1998* (NSW).

65. Please read: NSW State Records' strategies for managing social media information.

Personal use of social media

66. 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.

67. As an employee of the IPC and the NSW Government, there is, however, a risk of legal and reputational damage (directly or indirectly and accidentally as well as with intention). This may occur to your person, as an employee within the IPC or to the IPC.

Non-compliance

68. All IPC employees are required to comply with this policy. Depending on the circumstances, non-compliance with this policy may constitute a breach of employment or contractual obligations, misconduct (under the IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees), sexual harassment, discrimination, or some other contravention of the law.
69. Those who fail to comply with this policy may face disciplinary action and, in serious cases, termination of their employment or engagement. In extreme cases, civil and/or criminal sanctions may be applicable.

Conduct while off duty

70. As members of a public sector organisation all employees must, even when off duty, act in accordance with the law and the content of this code. In so doing employees must ensure that they do not bring discredit to themselves as private citizens or to the IPC, and that they model exemplary behaviour and act as a positive influence in the community.
71. Employees should be aware that unlawful or unprofessional conduct, even in a private capacity, which may damage, or has the potential to damage, the reputation of the IPC, may constitute misconduct and attract action by the IPC in accordance with section 69(4) of the *Government Sector Employment Act 2013.*
72. Section 69(1) of the *Government Sector Employment Act 2013* provides that action can be taken for misconduct which occurs when an employee is off duty or before his or her employment.

Public comment

73. Public comment is any comment made where it is expected that it will be seen or heard by members of the public. This includes comments made on social networking sites (such as "Facebook," "Instagram," "LinkedIn," "YouTube" and "Twitter"); on the internet, including media-related websites and independently published blogs that invite public comments.
74. As a private individual, employees have the right to participate in public debate on political and social issues. In exercising this right, they also have the responsibility to make it very clear they are speaking as private individuals and not representing the official views of the IPC or the NSW Government.

    In participating in any political, community and personal activity, employees must:

    - ensure that all content published is factually accurate and not misleading and complies with relevant legislation and IPC policies;
    - not make any comment where it could be inferred that the public comment, although made in a private capacity, is in some way an official comment of the NSW Government or of the IPC;
    - not upload, post or comment on IPC information before official announcements have been made;
    - not make comments or perform any online actions (such as liking) that would bring the IPC into disrepute or embarrass the agency;
    - not use information obtained through their work at the IPC to assist their political, community or personal activities, or make the information known to any other person; and

- not misrepresent the position of the IPC on any issue.

75. For further information please read IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees.
76. Employees must not use the IPC's internet and computer resources to provide comments to journalists, politicians and lobby groups other than in the course of their official duties and as approved by the IPC.
77. The IPC's Media Policy outlines circumstances where it is and is not appropriate to make comment to media. Employees must not approach the media on IPC-related matters or discuss IPC business with the media unless authorised to do so by the Manager, Communication & Corporate Affairs.

Using social media for unauthorised investigations

78. Staff who are not individually authorised by their business area manager to conduct investigations (for example into complaints) must not conduct independent investigations via social media. If an employee witnesses or suspects any inappropriate behaviour, they must report it to their business area manager who will forward it to the appropriate team for further investigation.

Identify as an IPC employee online

79. If an employee identifies as an IPC employee on their personal social media accounts, they must be mindful that in their public life, they are required to serve the government of the day in an impartial manner. As LinkedIn is a professional networking platform, user's employment is usually stated and sections 21 to 56 apply.
80. It is recommended that social media engagement relating to IPC services be limited to 'Reactions' (such as Likes), Sharing of content, and Tagging of online acquaintances, when deemed appropriate. When engaging with online content caution is expected.
81. This policy does not stop employees from commenting on public posts but recommends caution and neutrality in tone.
    - Example, bias: strongly agreeing or disagreeing with a policy announcement can be perceived as bias.
    - Example, neutral: sharing information about an officially endorsed program as a link or post with a simple statement such as "this may interest all the law students I know" is appropriate.
    - Example, staff support: congratulating staff on work related achievements, such as winning a Premier's Award. Avoid commenting on the program or their specific duties; rather focus on acknowledging the achievement.

People who do not identify as an IPC employee online

82. People who do not identify themselves as an IPC employee when posting online are considered to be commenting in a private capacity under this policy and must comply with section 93 of this policy.
83. Staff should be aware that they can be identified as an employee of the IPC from their online activities. For this reason, staff should not post about their work, colleagues in context of work, or official information that provides employee related insights. Any identifiable information can be deemed in violation of the IPC Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees.

84. Employees must also be mindful of the subject matter and tone of their comments on public social media, ensuring that any comment made is not referrable to the IPC and does not bring discredit to the IPC.

Professional networking platforms

85. Social media platforms such as LinkedIn provide employees with the opportunity to professionally network and share best practice information. While profiles on professional social networking pages are usually made as private citizens, personnel who identify themselves as employees and are commenting on matters relating to the IPC are commenting in an official, not a private capacity and so must comply with sections 21 to 56 of this policy.

Security on professional networking platforms

86. Limit information on professional networking platforms like LinkedIn to career related content. Avoid updates that show non-related travel, for example, as these platforms are targeted by scammers, organised crime (e.g. outlaw motorcycle gangs) and terrorist groups.

Employees representing a union

87. Comments made on matters relating to union business by members of unions in their capacity as a local delegate within the IPC or by union office holders employed by the IPC 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 IPC. An employee representing a union must adhere to the IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees.

Online access

88. 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 this policy, the IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees.

Privacy

89. People's personal information is important. When using social media, it is crucial to remain vigilant and regularly check your privacy settings to keep your information safe. This includes changing privacy settings, so they are only viewable by friends and family and only disclosing online location to trusted individuals.

90. It is recommended that personnel avoid using their full name and do not mention the location of their workplace.

91. The IPC recommends visiting the Stay Safe Online website to access tips for effective privacy online. Please visit Manage Your Privacy Settings for links on how to change your social media security settings. https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/

92. Staff should familiarise themselves with password security procedures for official IPC accounts and be equally as cautious with their private accounts. The Information and Cyber Security Group recommends changing passwords on a regular basis and adding Multi Factor Authentication that requires an additional form of authentication every time you sign in from a new device.

Code of Ethics and Conduct, checklist

93. Employees must adhere to the IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees 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 IPC or the NSW Government, nor give the impression that their views express those of the IPC or the NSW Government
- commit the IPC to any action or initiative unless authorised to do so
- refer to pending court proceedings to avoid publishing material that may prejudice those proceedings or breach a court suppression order
- 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 or information acquired in the workplace or while on duty including and especially relating to colleagues and clients
- make comments or perform any online actions (such as liking) that would bring the IPC into disrepute or embarrass the agency
- check-in online when at work as disclosing your location while at work is considered risky behaviour
- use social media in the workplace in a way that allows identification of their location where this creates risk for the individual or the IPC
- 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 IPC's Code of Conduct and NSW Public Service Commission's Code of Ethics and Conduct for NSW government sector employees.
- 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
- disclose IPC email addresses or use any IPC logos or insignia
- use the IPC email system for any personal postings or interactions over social media platforms
- use their IPC issued email address to create a personal social media account.

Legislative Context

- *Anti-Discrimination Act 1977* (NSW)
- *Government Advertising Act (2011)* (NSW)
- *Government Information (Public Access) Act 2009 (GIPA Act)* (NSW)
- *Government Sector Employment Act 2013* (NSW)
- *Government Sector Employment Regulation 2014*
- *Health Records and Information Privacy Act 2002 (HRIP Act)* (NSW)

- *Privacy and Personal Information Protection Act 1998 (PPIP Act)* (NSW)
- *State Records Act 1998* (NSW)

Related Policies

This Policy is informed by the IPC, state and federal policies and guidelines including:

- Australian Cyber Security Centre (ACSC) Security and Safety Tips for Social Media
- Australian Cyber Security Centre (ACSC) Passphrase Requirements
- NSW Government Digital Strategy
- NSW Government Open Data Policy
- NSW Government Advertising Guidelines
- NSW Government Advertising Handbook
- NSW Government Social Media Policy and Guidelines
- NSW Government Brand Guidelines issued by the NSW Department of Customer Service
- NSW Public Service Commission Code of Ethics and Conduct for NSW government sector employees
- IPC Code of Conduct
- NSW Department of Customer Service Acceptable Use of Information and Information Systems Policy
- NSW Ombudsman, *Applying the commitments to effective complaint handling - guidance for agencies*
- NSW Ombudsman, February 2017, *Effective complaints handling guidelines*
- NSW Ombudsman, June 2015, *Complaint management framework*

Definitions

Administrator is an IPC employee who manages the technical details of establishing the social media channel. The Communications and Corporate Affairs Communications team appoints Administrators. Administrators can 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 IPC in that division or agency's social media. Social Media Procedure 6.1 details the approval process for staff undertaking this role.

Business area manager is an employee Director, who has administrative responsibility for their business area.

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 Customer Service NSW

IPC means the Information and Privacy Commission NSW.

IPC's Code of Conduct refers to the IPC's existing Code of Conduct. A code of conduct is a guide to ethical workplace behaviour, setting out the minimum standards expected of employees of the IPC. It applies to all aspects of employment, including the workplace environment and workplace activities, and provides an ethical framework for decisions, actions and behaviour.

Media Policy refers to an employee's relevant existing Media Policy and includes the NSW Department of Customer Service's Media Policy.

Employee means employee of the IPC and persons engaged to provide the IPC with services, information or advice. Employees are public service employees within the meaning of Part 4 of the *Government Sector Employment Act 2013* and include ongoing, temporary, casual, trainee, ministerial staff, SES officers, contractors, non-judicial statutory appointments and any member of the public service.

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 IPC 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 an IPC representative.

Sharing tools are tools such as 'add this' share', 'retweet' or 'repost' 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 (e.g. Facebook, LinkedIn, Yammer, Weibo)
- video and photo sharing websites (e.g. Flickr, YouTube, Instagram, Vimeo, Vine)
- blogs, including weblogs, corporate blogs and personal blogs
- blogs hosted by media outlets (e.g. 'comments')
- micro-blogging (e.g. Twitter)
- wikis and online collaborations
- forums, discussion boards and groups (e.g. Google groups, Yahoo! Groups, Reddit)
- Vlogs and podcasting
- instant messaging including SMS (e.g. 'WhatsApp')
- geo-spatial tagging (e.g. Foursquare, Yelp, Snapchat)
- live broadcasting apps (e.g. Periscope, Facebook LIVE)
- review pages (e.g. Yelp, Zomato)
- online encyclopaedias (e.g. Wikipedia)
- any other channels or tools that allows for creation and exchange of user generated content.

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.

Document Information

Title	IPC Social Media Policy
Document number	D19/468496/DJ
Policy owner	Manager, Communications & Corporate Affairs
Classification	IPC Corporate Policy
Keywords	social media; social network; communication; online privacy; cyber security; administrator; digital communication; privacy; code of conduct
Applicability	Whole of IPC application

Version	Date	Reason for Amendment
1.1	27/11/2019	Initial draft
1.2	24/04/2020	Updates following 2019 Machinery of Government changes.
1.3	29/06/2021	Reviewed

Contact Email	Contact Phone	Date Issued	Next Review date
communications@ipc.nsw.gov.au	1800 472 679	24/04/2020	30/06/2022