

Social Media Policy

13 June 2023

Version 2

Document information

Document name:	Social Media Policy	Type of document:	Policy
Status:	Active	Version number:	2
Date originally created:	12 May 2022	File reference:	ADM/8470
Superseded policy:	Media policy, social media policy	Compliance:	All staff
Related policies/ documents:	Code of Ethics and Conduct	Publication date:	13 June 2023
Review date:	13 June 2025	Policy owner:	Chief Operating Officer
Distribution:	Public	Feedback:	Legal, Governance and Risk Branch

NSW Ombudsman

Level 24, 580 George Street
Sydney NSW 2000

Phone: (02) 9286 1000

Toll free (outside Sydney Metro Area): 1800 451 524

Website: ombo.nsw.gov.au

Email: nswombo@ombo.nsw.gov.au

© State of New South Wales

Contents

1.	Introduction and overview	1
2.	Application	1
3.	Related policies	2
4.	Key principles	2
5.	Terms and Concepts	2
	Use of social media in Ombudsman functions.....	3
	Ombudsman officers' use of personal social media	3
	Questions about social media use	6
6.	Ombudsman approval	6

1. Introduction and overview

This Policy governs the personal use of social media by Ombudsman officers (**officers**).

Its primary aim is to ensure that, in respect of all communications that are or may become public:

- we maintain public confidence and trust, by upholding our values of integrity, impartiality, fairness, transparency, professionalism and respect, and
- any public views expressed are those of the Ombudsman and the Office, and not the views or opinions of individual officers.

The Policy acknowledges and respects the rights of officers to engage with social media and to express personal and political views and opinions. At the same time, those rights must be balanced with their status as an officer of the NSW Ombudsman and their duty to ensure that their social media activity (including on personal accounts and in non-work time) does not undermine public confidence and trust in themselves or the NSW Ombudsman.

The NSW Ombudsman is an independent office established by Parliament, whose functions include the exercise of extraordinary statutory powers of investigation, and the public expression of conclusions, findings and recommendations about the conduct of government agencies, public officials, community service providers and others. In those circumstances, maintaining public confidence and trust (e.g. that those functions are always exercised independently and impartially in the public interest, and that opinions are always based only on credible evidence following due investigation or inquiry) may be even more important than in the case of other public service agencies. This public confidence and trust may also be more liable to be damaged by unauthorised or inappropriate public views and comments expressed by officers.

This Policy also recognises that, on social media:

Our private actions can have far wider-reaching effects than we intend—or, often, can control. Our online footprint is effectively permanent, and what we post can find its way to people we never imagined would see it . . . [w]e cannot always predict what will go viral, nor how our posts might be taken out of context.¹

2. Application

The Policy applies to all officers both when carrying out work functions **and in their private capacity and during their private time**.

In respect of conduct on social media activity, the Policy applies only to conduct of an officer that occurs on or after 12 May 2022.

This Policy does not have retrospective effect. This means that where an officer's social media activity, including the posting of content, occurred before this date:

- that activity is not to be taken to be a breach of this Policy (although it may, depending on the circumstances, have been a breach of the Code of Ethics and Conduct or other Ombudsman policy that was in force at the time)

¹ Social media: Guidance for Australian Public Service Employees and Agencies, Australian Public Service Commission, September 2020

- the officer will not be held responsible for any use of, or activity relating to, that activity (including earlier content posted by them) by someone else who is unconnected to the officer.

However, the Ombudsman may, if it is reasonable to do so, direct the officer to take necessary steps to ensure that particular content or activity that occurred before the date of this policy aligns with this policy going forward (e.g., by directing that particular content be removed or made non-public). A failure to comply with that direction would be a breach of this Policy.

3. Related policies

This Policy applies in addition to the Office Code of Ethics and Conduct.

This Policy deals with social media activity that is or might be attributed to, or might otherwise reflect on the reputation or standing of, the Office. There are a range of privacy, non-disclosure and personal conduct obligations that apply to this activity, in the same way that they apply to other activities undertaken by officers. These are set out in the Code of Ethics and Conduct and the Privacy and Information Management Framework.

Officers are also required to comply with Ombudsman policy relating to the use of Ombudsman IT devices and applications.

See also the Ombudsman's Media policy, which outlines how the Ombudsman's office deals with media queries and the Ombudsman's official social media accounts.

4. Key principles

- I. Comments relating to the Office, its functions and activities may only be made by the Ombudsman or a person authorised by the Ombudsman to comment.
- II. Officers are entitled to use social media in their private capacity during non-work time, but that use must comply with this Policy, the Ombudsman Code of Ethics and Conduct and their terms of employment. Officers must avoid using social media in a way that could damage public confidence or trust in the Ombudsman or the Office.
- III. Legally, any content on a social media site that is licensed to or controlled by an officer is treated as if it were published by that officer, regardless of who posted the content or even whether the officer is aware of that content. This means officers must take care to also moderate material that may be posted to their social media page by others.

5. Terms and Concepts

Officer means any person working in the Office, including any Deputy Ombudsman, senior executive or anyone employed under the *Government Sector Employment Act 2013*, as well as any agency or temporary staff, intern or contractor engaged by the Office to carry out Ombudsman activities.

Social media site means any electronic forum on which users and/or the public can post or otherwise contribute to content and includes:

- (a) platforms such as Facebook, Instagram, LinkedIn, YouTube, Twitter and TikTok

- (b) sites that permit user contributions or interaction such as websites, comments sections in news articles, blogs, chat rooms and wikis, and
- (c) group email chains or messaging applications (except where all of the participants are personally known to each other and where the circumstances of the communication are such that there is a shared expectation of no further dissemination).

Use of social media by an officer includes posting or otherwise contributing to content on a social media site, regardless of whether that site is considered ‘private’ or ‘closed’ to the general public or its access is ‘restricted’ in any other manner. Use could include posting content, uploading pictures, participating in online petitions or fundraisers; commenting on posts, photos, or videos; sharing memes; ‘liking’ or posting an emoji or other reaction to content posted by other; and sending direct or private messages on social media sites.

Use of social media in Ombudsman functions

Officers are not permitted to use social media accounts (whether their own or the office’s) for any investigative, review, auditing or monitoring purposes (for example, to obtain information relevant to an Ombudsman function) unless:

- that information is accessible to any member of the public, and is not information available only to relevant social media account holders, or
- that use is permitted by the Ombudsman or Chief Deputy Ombudsman in writing.

Ombudsman officers’ use of personal social media

Officers have a right, in their personal lives, to participate in political and community activities, to pursue private interests, and to personal and professional expression. This includes a right to participate, as individuals, in online discussions about a range of social and political issues.

However, this right must be balanced with their status and obligations as an officer. Personal behaviour (including during non-work time) can undermine public confidence and trust. Accordingly, the obligations in this Policy apply at all times.

Officers may only use social media for personal use in non-work time.

Officers must not use social media if doing so:

- would, or would reasonably be perceived to, interfere with their official duties
- would, or would reasonably be perceived to, conflict with their duty as a public servant within an independent statutory office to undertake their work in a politically neutral manner and to make fair and impartial decisions
- would give rise to any conflict of interest (actual, perceived or potential)², or

² Social media comment would not ‘give rise’ to a conflict of interest if it relates to an already existing conflict of interest that has been fully disclosed and is being appropriately managed in accordance with the Office Code of Ethics and Conduct. For example, an officer who has a family member who is a client of a community service provider will have a conflict of interest with respect to the Ombudsman’s oversight of that provider. To manage that conflict, the officer may be required not to be involved in any Office work that involves that provider. In managing the conflict, the officer may be further authorised to participate in social media activity in relation to the relevant provider in a way that another officer (who does not have a disclosed and managed conflict) would not. However, even in these circumstances the conflicted officer must comply with the other requirements of this Policy, for example by ensuring that any social media activity in respect of the provider is not perceived as being made in an official capacity or otherwise as representing views of the Office.

- otherwise has the likely effect, or purpose, of damaging the reputation of, or public confidence and trust in, the officer, the office or the Ombudsman.

An example of how use of social media may damage reputation or public confidence and trust is where it leads an ordinary member of the community to question the capacity of the officer, office or Ombudsman to:

- act only in the public interest and without regard to any private or political views
- behave at all times in accordance with the values of integrity, impartiality, independence, transparency, professionalism and respect.

Understanding and assessing the risks – taking a cautionary approach

The NSW Ombudsman is an independent office established by Parliament, whose functions include the exercise of extraordinary statutory powers of investigation, and the public expression of conclusions, findings and recommendations about the conduct of government agencies, public officials, community service providers and others.

In those circumstances, maintaining public confidence and trust (e.g. that those functions will be exercised independently and impartially in the public interest) may be even more important than in the case of other public service agencies. Moreover, that public confidence and trust may be more liable to be damaged by unauthorised or inappropriate public views and comments expressed by officers.

Key factors that can particularly heighten the risk that social media activity will damage public confidence and trust in the Ombudsman's office include:

(a) The officer's seniority

Generally speaking, the more senior an officer, the greater the risk of their online behaviour affecting public trust and confidence in the office. Senior officers set the tone for the office and should be relied upon to act as an exemplar to other staff and broader networks. However, given the particular status and functions of the Ombudsman and all of its officers, the risk exists for all officers at all levels.

(b) The relationship between the post or other content involved in the use of social media and the office or its functions or work

Content that refers or relates to the Ombudsman or the office, or to persons or bodies within our jurisdiction, is inherently riskier than content that is unconnected with Ombudsman functions. However, officers should bear in mind that members of the public who view social media activity will not necessarily know the scope of the Ombudsman's functions, or be able to tell which entities the Ombudsman can and can't investigate or oversight.

(c) The nature and degree of views or opinions expressed or implied

The risk to public confidence and trust is greater the more extreme the behaviour or expression, including the tone and language of posts. The expression of strong criticism or endorsement may be more likely to lead an ordinary member of the community to doubt whether the officer would be able to put aside their personal views and act professionally and impartially in their work. Derogatory, threatening or abusive comments, even about unrelated topics, can also damage perceptions of professionalism, integrity and respect and the reputation of the office.

(d) The type of social media

Personal online activity is more likely to be associated with the Ombudsman when that activity appears on professional networking platforms, such as LinkedIn, where the nature of the platform inherently connects the account owner with their employer.

Other factors to consider are that the nature of social media exacerbates the chances of a message being misconstrued, misunderstood or taken out of context, and that, in most cases, the message can be difficult, if not impossible, to erase.

Anonymous posting

While the risks of social media use are greater if the officer is identified as an officer of the NSW Ombudsman, it is not eliminated merely because an officer is not identified as such. Officers can be identified online in a range of ways, even if they post anonymously or are using an alias – and once identified as an officer, the use of social media can affect reputation and public confidence regardless of any intention of the officer to keep that use separate from their role or work with the office.

Officers who post anonymously should assume that at some point their identity and the nature of their role with the office may be revealed.

Privacy settings

Privacy settings are designed to control who can see and respond to social media content. Privacy settings are not capable of eliminating all risk of inappropriate social media use, and are not a substitute for avoiding social media use that might impact on public confidence or trust in the independence and objectivity of the Office. However, officers are encouraged to check and, if appropriate, modify, those privacy settings on their social media accounts. In the event of an issue arising about social media use, an officer will be presumed to know what privacy settings apply to their own social media account.

Officers must also be aware that, even in a private or closed setting, there is a very real risk that someone who can access social media activity may disseminate that material beyond the audience for which it was intended. Where that activity is disseminated, the officer may not be able to rely on an ‘implicit understanding’ that the content remain within the group to whom it was communicated.

Disclaimers

In some cases, such as professional networking sites such as LinkedIn, where an officer’s association with the NSW Ombudsman will be disclosed, it may be useful to include a disclaimer on a profile or post to indicate that views are a person’s own and do not represent the Ombudsman or the office.

However, a disclaimer does not eliminate all the risks. Public confidence and trust can still be damaged by an officer’s behaviour even if the officer states that they are acting in a private capacity.

Liking, sharing, following, friending, and tagging

‘Liking’ a post carries similar risks to posting material, as it might reasonably be perceived as an endorsement of the content – even if that is not the officer’s intention.

This risk also applies, and perhaps more so, to ‘sharing’ content.

‘Sharing’ a post together with commentary (whether positive, negative or neutral) is tantamount to posting and the same considerations as set out above to posting need to be considered. Officers should never ‘share’ content they would not post themselves.

'Following' or 'friending' is generally low risk, and risks will arise only to the extent that the officer then engages with content.

Being 'tagged' in a post can carry some risk of being seen as associated with or endorsing content. If an officer is tagged in a post that they themselves would not post, it would be prudent for them to untag themselves and consider asking the person not to tag them again.

Comments by others

Legally, content posted to a social media account held or controlled by a person is taken to be the responsibility of that person, regardless of who posts or contributes to that content and whether or not the person is aware of that content.

Officers should therefore take steps to ensure that any content posted by others on their social media accounts (i.e. things that are posted to their 'page' or comments that are made in threads responding to their posts) does not place the officer in a position of contravening this policy.

Factual information

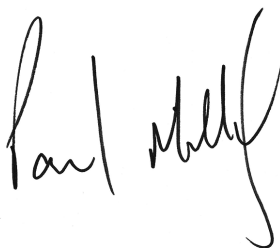
Nothing in this Policy prevents Ombudsman officers from identifying, in a LinkedIn account or similar forum, that they are (or have previously been) employed by the Office and the capacity in which they are employed, provided the information is factually accurate.

Officers are also welcome to 'share', 'like' or 'follow' content published on the Office's social media accounts. However, the Office will not require or request officers to do so, and will not encourage them to otherwise comment publicly on work of the office on social media.

Questions about social media use

If you have any questions about whether any of these activities create a risk, you should raise them with the Legal, Governance and Risk Branch.

6. Ombudsman approval



Paul Miller
NSW Ombudsman