



Social Media Policy - Employees and Councillors

Policy No:	1.27
Approved by Council:	August 2026
New Review Date:	August 2028
Minute No:	C258/15-2026
ECM File No:	12.298
Version:	1.0
Responsible Officer:	Communications Lead
Strategic Plan Reference:	5.2 Council is a desirable place to work

1. POLICY STATEMENT

- 1.1 Kingborough Council recognises the opportunities social media provides to engage in meaningful, two-way communication with the community.
- 1.2 Social media is one of the communication tools, service avenues and consultation methods used by both employees and councillors to improve access to and delivery of Council's key services.
- 1.3 Council also acknowledges the organisational value offered by social media for networking, recruitment, professional development, employee engagement, collaboration and innovation.
- 1.4 This policy provides guidance to employees and councillors on communicating with the community through social media where reference is made, directly or indirectly, to Kingborough Council, its operations, decisions, services, or community matters connected to the organisation.

2. DEFINITIONS

- 2.1 **Social media** means internet and mobile based platforms for creating, sharing, and discussing content (e.g. Including but not limited to: Facebook, Instagram, LinkedIn, YouTube, X/Twitter, blogs, forums).
- 2.2 **Authorised Officer** means an employee authorised by Council's Chief Executive Officer to post, moderate, or respond on behalf of Council on social media.
- 2.3 **Administrator** means a person with account management access to official Council social media channels.
- 2.4 **CEO** means the Chief Executive Officer being the General Manager as appointed by the Kingborough Council pursuant to section 61 of the *Local Government Act 1993* (TAS).

3. OBJECTIVE

This policy aims to:

- 3.1 Provide clear expectations for professional and personal use of social media.
- 3.2 Promote appropriate and responsible use of social media.
- 3.3 Promote an informed approach to social media use to minimise the risk of spreading misinformation or misuse.
- 3.4 Protect and enhance the reputation of Council.
- 3.5 Manage risks, including legal, reputational, and operational impacts from social media use.
- 3.6 Promote a safe and positive online environment.

4. SCOPE

- 4.1 This policy applies to the individuals listed below, when initiating or responding to communications with the community via social media, where reference is made, directly or indirectly, to Council, its operations, decisions, services or community matters relating to the Council.
- 4.2 Who:
 - 4.2.1 Employees regardless of whether they work full-time, part-time or casual.
 - 4.2.2 Councillors (elected members).

4.3 When:

- 4.3.1 Both professional and personal use of social media, whether during work or personal time, and whether accessed via Council-owned or personal devices, where the content relates to Council business, Council employees, Councillors, Council decisions, Council services, Council resources, or a person's role with Council.
- 4.3.2 This Policy does not seek to regulate purely private social media activity that has no connection to Council. However, personal social media activity may fall within this Policy where it refers directly or indirectly to Council matters or may reasonably affect Council's reputation, governance, legal obligations, workplace relationships, employee wellbeing or public confidence in Council.
- 4.3.3 Corporate use when posting, commenting, or managing official Council social media accounts.

5. PRINCIPLES

- 5.1 All social media activity relating to the scope of this document must:
 - 5.1.1 Be accurate and respectful; information must be factual, professional, and courteous.
 - 5.1.2 Uphold Council values as per Council's Strategic Plan.
- 5.2 Protect confidentiality:
 - 5.2.1 Do not disclose sensitive or confidential information that has been acquired through oral discussions, email or Council documents as defined in the Employee Code of Conduct Administrative Policy section 3 and the Local Government Code of Conduct and Councillor Workshop Policy.
- 5.3 Be relevant and relate to Council services, activities, or important community information (Communications and Engagement Policy 1.3).
- 5.4 Avoid conflicts of interest; declare and manage any potential conflicts (Employee Code of Conduct 3.3 & Councillor Local Government Code of Conduct).
- 5.5 Comply with any applicable laws including but not limited to defamation, privacy, copyright, WHS and anti-discrimination (see section 10).
- 5.6 Nothing in this Policy prevents Councillors from scrutinising Council performance, advocating for constituents, expressing disagreement with Council decisions, or participating in public debate. Councillors are elected representatives and may comment on Council decisions, processes, services and performance. However, Councillors are expected to do so in a way that is lawful, accurate, respectful and consistent with the Councillor Code of Conduct. Public comment should be directed at Council decisions, processes, services or performance rather than personally targeting individual Council employees.

6. PROCEDURE

6.1 Councillors:

- 6.1.1 Not engage in or encourage behaviour that breaches this policy.
- 6.1.2 Ensure that social media use complies with the Local Government Code of Conduct, applicable laws, and relevant legal and risk considerations outlined in section 11.

6.1.3 When expressing views about Council-related matters in a personal capacity, Councillors must clearly state that the views expressed are their own and are not the official position of Council, unless the Councillor is expressly authorised to speak on behalf of Council.

6.1.4 A suitable disclaimer is:

“The views expressed are my individual comments and opinions, not the official position of Council.”

6.1.5 Are not to use social media to influence decisions in which they have a conflict of interest or to pre-empt a Council decision.

6.1.6 Must not publish content about Council employees, Councillors or Council business that is personal, offensive, inflammatory, bullying, harassing, defamatory, discriminatory or intentionally disparaging.

6.1.7 Must comply with any reasonable direction issued by the Chief Executive Officer to amend or remove social media content that is determined to be in breach of this policy.

6.1.8 Where social media content published, shared or controlled by a Councillor creates a real or foreseeable risk to the health and safety of Council employees, Councillors or other persons, the Chief Executive Officer may request that the content be removed, amended or corrected. Such a request will be made having regard to Council’s obligations under the *Work Health and Safety Act 2012* and associated WHS incident management processes.

6.1.9 Where content does not raise a workplace health and safety concern, but appears inconsistent with this Policy, the Councillor Code of Conduct, confidentiality obligations, privacy requirements, defamation law or other governance obligations, the Chief Executive Officer may request that the Councillor amend or remove the content.

6.1.10 If the matter is not resolved, it may be managed through the applicable statutory, Code of Conduct, workplace health and safety, legal or governance process

6.1.11 Must not establish or use fake, anonymous or misleading accounts, identities or third-party arrangements to deceive others about Council business, Council processes, Council identity, or the person’s authority or role in relation to Council.

6.1.12 Must not disclose confidential or internal information, including any content acquired through staff emails, unless it has been explicitly approved for public distribution.

6.1.13 Must not use Council branding or intellectual property without permission.

6.2 Managers/supervisors:

6.2.1 Promote this policy within their area of responsibility.

6.2.2 Address potential policy breaches promptly and appropriately (see section 7).

6.3 Employees:

6.3.1 Are not to engage in or encourage behaviour that breaches this policy.

6.3.2 When performing official duties, ensure that your use of social media does not violate applicable laws.

6.3.3 Must comply with any reasonable direction issued by the Chief Executive Officer to amend or remove social media content that is determined to be in breach of this policy.

6.3.4 Must not establish or use fake, anonymous or misleading accounts, identities or third-party arrangements to deceive others about Council business, Council processes, Council identity, or the person's authority or role in relation to Council.

6.3.5 Must not publish content about Council employees, Councillors or Council business that is personal, offensive, inflammatory, bullying, harassing, defamatory, discriminatory or intentionally disparaging.

6.3.6 Must not tag work colleagues into posts, comments, or discussions on official Council social media platforms.

6.4 Authorisation

6.4.1 All corporate accounts must be approved by the Communications Lead or the CEO.

6.4.2 Only Authorised Officers may post, respond, or moderate on behalf of Council.

6.4.3 The CEO can implement additional operational procedures relating to Council's use of social media without amending this policy.

6.5 Emergency Communication

6.5.1 Individuals covered by this Policy must not create or publish original content relating to any emergency incident, natural disaster or public safety matter unless authorised or instructed by the Municipal Emergency Management Coordinator, the Chief Executive Officer, or another authorised emergency management authority.

6.5.2 Councillors and employees may share official Council communications or information issued by authorised emergency service agencies to support coordinated public messaging. Care must be taken not to speculate, duplicate unverified information, or publish content that may conflict with official emergency communications.

6.6 Content Standards

6.6.1 Authorised Officers:

- i. Use approved branding, logos, and style guidelines.
- ii. Must remain politically neutral, factual and consistent with adopted Council positions.
- iii. Must ensure official Council channels are not to be used to promote, endorse, advantage or disadvantage any Councillor, candidate, political party, campaign group or election position.
- iv. Credit original sources and comply with copyright requirements.
- v. Be factual and relevant to the topic.
- vi. Do not use abusive, obscene, defamatory, or discriminatory language.

6.6.2 Councillors:

- i. Do not use branding, logos, unless performing official duties.
- ii. Credit original sources and comply with copyright requirements.
- iii. Do not use abusive, obscene, defamatory, or discriminatory language.

6.7 Responding to the public

6.7.1 Authorised Officers:

- i. If a response is required, ensure that this is delivered promptly, professionally, and courteously.
- ii. Direct service requests, complaints, or formal submissions to official Council channels.
- iii. Avoid engaging in arguments or debates.
- iv. When referring to Council employees in social media content about Council matters, positions, titles, business units or official roles should be used rather than personal names.
- v. Council employees must not be named, tagged, photographed, identified or otherwise personally referenced unless authorised, required for official Council business, already approved for public release, or otherwise lawful and appropriate in the circumstances.
- vi. Implement a risk-based strategy for comment moderation (see section 7).

6.7.2 Employees: (excluding Authorised officers) must not:

- i. Provide advice on behalf of Council to public comments.
- ii. Must not tag work colleagues into posts, comments, or discussions on official Council social media platforms to avoid exposing individuals to online abuse, unintended identification in sensitive matters, or confusion about Council positions and responsibilities.

6.7.3 Councillors:

- i. When making any reference, direct or indirect, to Council, its operations, staff, or procedures, Councillors must follow the principles outlined in Section 5 of this Policy. This ensures consistency, professionalism, and compliance with established guidelines.
- ii. Direct service requests, complaints, or formal submissions to official Council channels.
- iii. Council positions, titles, or official roles may be referenced; however, personal names must not be used.

6.8 AI – Artificial Intelligence

6.8.1 With the increasing availability and use of artificial intelligence (AI) tools to generate images, video, audio and written content, Council recognises the need to ensure AI-generated material used across social media and digital communication channels is accurate, ethical, transparent and does not mislead the community or undermine public trust in Council communications.

6.8.2 Councillors and Staff:

- i. All AI-generated imagery must be generic in nature and must not be capable of impersonation or being reasonably mistaken for identifiable Councillors, employees, or community members without their explicit prior consent.
- ii. AI-generated content including imagery and audio must not be used in a manner that could misrepresent Council operations, mislead the public, damage public trust, create reputational harm, or spread misinformation or deceptive content.

7. MONITORING AND EVALUATION

- 7.1 Social media content should never be assumed to be private, even where it is posted in a private or closed group. Content posted in private groups, closed pages, messaging groups or similar forums may be copied, screenshotted, forwarded or republished without the author's knowledge or consent.
- 7.2 Where such content relates to Council matters and creates legal, governance, reputational, privacy or workplace health and safety risks, it may be considered under this Policy.
- 7.3 This policy promotes a risk-based approach to moderation taking into consideration that:
 - 7.3.1 Corporate accounts will be monitored on business days during business hours or more regularly during emergencies.
 - 7.3.2 Corporate accounts may be monitored outside of business hours on occasion.
 - 7.3.3 The Communications team will track engagement metrics for quarterly and annual reporting.
 - 7.3.4 All corporate accounts must include an automatic message that tells people how often the account is checked and directs service requests or complaints to official Council channels.
 - 7.3.5 Administrators will maintain records of significant online interactions.
- 7.4 Authorised Officers will:
 - 7.4.1 Remove and/or block users who post content which are deemed to be illegal, offensive, discriminatory, defamatory, or misleading.
 - 7.4.2 Delete/hide spam, promotions, irrelevant links, content unrelated to the original social media post or Council activities.
 - 7.4.3 Delete/hide content breaching privacy, confidentiality, or platform terms of use.
 - 7.4.4 Where content may involve a threat, harassment, discrimination, defamation, privacy breach, confidentiality breach, staff targeting, legal risk or workplace health and safety risk, take reasonable steps to preserve a record of the content before it is hidden or removed.
 - 7.4.5 Content that is reasonably critical of Council, Council decisions, services, processes or performance will not be removed merely because it is critical. Such content may only be hidden, removed or moderated where it breaches this Policy, applicable law, platform rules, or creates a safety, privacy, confidentiality, defamation, discrimination or other material risk.
- 7.5 Councillors:
 - 7.5.1 Must be responsible for taking reasonable steps to moderate social media accounts, pages or groups they control where those channels are used for Council-related purposes in accordance with documents outlined in Section 9 and 10.
 - 7.5.2 This does not require continuous monitoring or guarantee that inappropriate comments will never occur. However, Councillors should act within a reasonable time after becoming aware of content on their account, page or group that may be unlawful, defamatory, discriminatory, harassing, privacy-breaching, confidential, threatening, misleading, personally targeted at Council employees, or otherwise inconsistent with this Policy.
 - 7.5.3 Where a Councillor becomes aware of content that may create a legal, governance or workplace health and safety risk, they should consider removing, hiding, correcting or

otherwise managing the content and, where appropriate, seek advice from the Chief Executive Officer or Communications Lead.

- 7.5.4 Must comply with any reasonable direction issued by the Chief Executive Officer to amend or remove social media content that is determined to be in breach of this policy.

8. TRAINING

- 8.1 Council will ensure all new employees and new Councillors receive a copy of this policy as part of their induction.
- 8.2 The Communications and People and Safety team will ensure that this policy is regularly communicated with all affected people covered by this policy.
- 8.3 That this policy is acknowledged by all affected employees and Councillors.

9. ENFORCEMENT AND BREACHES

- 9.1 Persons covered by this policy, who breach this policy may (as is appropriate and as applicable) be subject to appropriate disciplinary action.
- 9.2 Employees and Councillors who observe any social media content that may contravene this policy should immediately report the perceived breach to their manager or the Communications Lead (in the case of employees) or the CEO (in the case of Councillors) for investigation and appropriate action.
- 9.3 Legal responsibility for social media content will depend on the circumstances and applicable law. Content published on personal social media accounts may expose the individual, and in some circumstances Council, to legal, governance, reputational or workplace health and safety risk.
- 9.4 Serious breaches may:
- 9.4.1 Expose individuals to legal proceedings; and
- 9.4.2 Make Council vicariously liable for the conduct of others.
- 9.5 Reporting of Breaches:
- 9.5.1 Employees and Councillors who observe any social media content that may contravene this policy should immediately report the perceived breach to their manager or the Communications Lead (in the case of employees) or the CEO (in the case of Councillors) for investigation and appropriate action.
- 9.6 Employee:
- 9.6.1 Breaches may result in disciplinary action under Council's Workplace Behaviour Administrative Policy 9.20, *Work Health and Safety (WHS) Act 2012* and the Employee Code of Conduct Administrative Policy 9.14.
- 9.7 Councillors:
- 9.7.1 Breaches by Councillors may result in action under the applicable Councillor Code of Conduct, *Local Government Act 1993*, *Work Health and Safety Act 2012*, privacy, defamation, anti-discrimination or other relevant legal or governance processes.
- 9.8 Where social media content creates an actual or potential workplace health and safety risk, the matter may also be recorded and managed through Council's WHS incident management processes.

- 9.9 Where appropriate, Council may seek legal advice or refer a matter to an external authority, including WorkSafe Tasmania, Tasmania Police, the relevant electoral authority, or another regulator.

10. LEGAL AND RISK CONSIDERATIONS

- 10.1 All persons covered by this Policy must comply with applicable laws, regulations, codes, Council policies and lawful directions relevant to their role or circumstances. Relevant legal and risk considerations include, but are not limited to:

10.1.1 Defamation: You may be found to be liable for any defamatory comments you post or allow to remain visible.

10.1.2 Privacy: Do not disclose personal or sensitive information including identifying employees by name (refer to the *Personal Information Protection Act 2004*).

10.1.3 Copyright: Obtain permission before using protected material.

10.1.4 Anti-discrimination: It's unlawful to treat someone unfairly or harass them because of attributes such as race, gender, disability, age, religion, or sexual orientation.

10.1.5 Contempt: Publicising court orders or matters under consideration by the courts.

10.2 Security:

10.2.1 Protect login credentials and be alert to phishing, malware, and other online risks.

10.2.2 Authorised Officers are to use 2 factor authentication when using login credentials and operating corporate accounts.

11. RELATED DOCUMENTS

- 11.1 Employee Code of Conduct Administrative Policy 9.14;
- 11.2 Local Government Code of Conduct;
- 11.3 Workplace Behaviour Administrative Policy 9.20;
- 11.4 ICT Usage Administrative Policy 9.2;
- 11.5 Disciplinary Administrative Policy 9.12;
- 11.6 Communications and Engagement Policy;
- 11.7 Customer Service Charter Policy 1.6;
- 11.8 Councillor Workshop Policy 1.19;
- 11.9 Code of Conduct for Councillors V4;
- 11.10 Work Health and Safety Policy V 4;
- 11.11 *Work Health and Safety Act 2012* (TAS).