

Social Media Policy Template

A guide to the responsible and safe use of social media

1. Overview

[Organisation Name] recognises that social media is an important tool for communication, engagement, and sharing information about our work. This policy sets out how social media should be used responsibly by staff, volunteers, and trustees, both in a professional capacity and in personal use where there is a connection to the organisation.

We aim to use social media in a way that is safe, respectful, lawful, and consistent with our values, while also protecting the organisation, its people, and those we work with.

2. Scope

This policy applies to employees, volunteers, trustees, contractors, and anyone posting content on behalf of the organisation. It covers both official organisational accounts and personal accounts where the organisation may be referenced or identified.

It is important to note that personal use of social media can still have an impact on the organisation where individuals are associated with it.

3. What We Mean by Social Media

Social media includes any online platform that allows users to create, share, and interact with content. This includes sites such as Facebook, X (formerly Twitter), Instagram, LinkedIn, TikTok, blogs, forums, and similar platforms.

4. General Principles

All social media activity connected to the organisation should be accurate, respectful, and lawful. It should reflect the organisation's values and support its mission, while maintaining appropriate professional boundaries.

Users should take care to protect confidentiality, respect privacy, and avoid any content that could cause harm to individuals, groups, or the reputation of the organisation.

5. Legal Responsibilities

All users must comply with relevant legislation when using social media. This includes the UK GDPR and the Data Protection Act 2018 in relation to personal data, as well as the Equality Act 2010 in relation to fairness and non-discrimination.

Users must also be mindful of laws relating to copyright, defamation, harassment, and safeguarding. Personal or sensitive information, including images or identifiable details, should not be shared without appropriate consent.

6. Responsibilities and Oversight

The organisation will ensure that responsibility for social media activity is clearly assigned. This may include designated staff or volunteers responsible for managing official accounts and content.

Only authorised individuals should have access to and post on official organisational channels. Where appropriate, training or guidance will be provided to support safe and effective use.

7. Use of Official Accounts

When using social media on behalf of the organisation, users should ensure that content is accurate, appropriate, and aligned with the organisation's purpose. Posts should be clear, inclusive, and reflect the organisation's tone and values.

Care should be taken to check information before it is published, and to respond to comments or messages in a professional and timely manner. Personal opinions should not be presented as organisational views.

Where images or stories involving individuals are shared, informed consent must be obtained in advance. Extra care must be taken when working with children or vulnerable adults, and the intended use of content should always be clearly explained.

8. Personal Use of Social Media

Individuals are free to use social media in a personal capacity but should be mindful of their connection to the organisation. It should be made clear where views are personal and not those of the organisation, for example through a disclaimer such as "views are my own".

Staff, volunteers, and trustees should avoid posting content that could reasonably be seen as damaging to the organisation's reputation or bringing it into disrepute.

Where an individual's role is publicly associated with the organisation, a higher level of care is expected in their online conduct.

9. Safeguarding and Risk

Social media must not be used to share confidential or sensitive information. Any safeguarding concerns identified through social media should be reported immediately through the appropriate internal processes.

Users should avoid engaging in public disputes or escalating online conflict, particularly where it involves the organisation or its stakeholders.

10. Brand and Reputation

Organisational branding, logos, and messaging should only be used where authorised. New accounts should not be created in the organisation's name without approval.

All social media activity should be consistent with the organisation's identity and values, helping to maintain a clear and professional public presence.

11. Managing Issues and Complaints

Social media channels should be monitored where possible to ensure appropriate engagement and to identify issues early. Comments and complaints should be handled proportionately and escalated internally where necessary, particularly if they involve reputational, legal, or safeguarding concerns.

12. Breach of Policy

Failure to follow this policy may result in action being taken, which could include removal of access to organisational accounts, internal disciplinary procedures, or further action where legal obligations have been breached.

13. Review

This policy will be reviewed regularly and updated where necessary to reflect changes in legislation, good practice, and emerging risks in the use of social media.

REVIEW DATE: