Social media

This page is from APP, the official source of professional practice for policing.

First published 23 February 2026

Forces may use social media for a wide variety of roles and purposes, including community engagement.

Roles and responsibilities

Social media is used across policing in a wide variety of roles and purposes. Forces require robust workflows between those roles, for the effective management of social media for public information and engagement.

Corporate communications

- Social media information asset owner (IAO).
- Social media management platform (SMMP) business product owner (BPO).
- Own the force social media strategy.
- Experts in public engagement, relevant legal and regulatory frameworks, mitigating and managing risk.
- May own the contractual relationship with the force's SMMP.
- Own the business continuity plans for corporate communications.

Contact

- May operate a dedicated 24/7 'digital desk' to triage and assess some, most or all of the force's official social media.
- Ensure that risk can be quickly identified and escalated to command and/or corporate communications.
- Respond to calls for service and intelligence submissions promptly and in line with **Contact management APP**.
- Maintain a safe and respectful environment by applying force community management standards.

Information management

- Set practices for compliant management of social media data, in accordance with the relevant legislation, including, but not limited to: Data Protection Act 2018, UK GDPR and NPCC National Retention Schedule (NRS).

Information security

- Lead on setting standards of security for the force's social media, and subject these to regular review.

Investigations and intelligence

- Manage the force's use of social media for investigative and intelligence purposes.

Neighbourhood or operational teams

- May be authorised to operate or contribute to the force's accounts (in line with local force policy) for hyper-local community engagement.
- May triage, assess and respond to community issues identified on force social media for their local area.

Professional standards department

- May be the owner of the force's social media policy, setting and enforcing standards, with other business areas acting as subject matter experts.

Social media strategy

Police forces are operationally independent and should make decisions on how to use social media locally to reach and engage their communities most effectively.

Communications officers should regularly review their choice and use of channels, including existing and new channels.

Communications officers should develop a dedicated social media strategy that should include:

- existing channel mix – how they are used and a future roadmap

- standards for content and accessibility
- an approach to collaborations with influencers, paid media and earned media alongside owned media
- community engagement and management standards and practices
- the required applications (‘apps’), software and hardware

The social media strategy may also include:

- specialist skills and capabilities required to deliver public engagement services
- training or continuing professional development (CPD) programmes to support the delivery of contact services and public engagement
- training or CPD programmes to support knowledge of the legal framework

Community management guidelines

Heads of communication should ensure their organisation has public-facing community management guidelines outlining the right to moderate user-generated content. This includes:

- removing posts
- blocking users
- taking action if rules are broken
- explaining why public comments may be hidden, deleted or restricted

Communications officers should:

- be aware of key platform algorithms and the related benefits of engaging with content, and the public
- have processes in place for rapid and appropriate escalation of potentially contentious or harmful online content – in most cases, authorised users should quickly identify content of this nature and escalate according to local processes
- consider resource provision for two-way engagement
- record the risk of not monitoring social media 24/7 if a force does not have the capability to do so
- make an informed decision on whether to operate private messaging
- have processes in place to manage surges in social media traffic
- consider using an SMMP
- make use of any native moderation controls offered by social media platforms or SMMP

- not use corporate social media engagement channels to contact, or attempt to contact, victims or witnesses who have not already engaged with the force using this channel

Security

To maintain security of social media accounts, forces should:

- protect their social media accounts using consistent branding and naming conventions on setup
- where possible, obtain official verification
- regularly monitor for fake and impersonation accounts
- report any fake or impersonation accounts to the relevant social media channel
- publish a list of all official accounts on the force website

Information security teams should lead on setting security standards for the force's social media. Standards should be regularly reviewed and, as a minimum, include:

- regular consultation between information security and the CCD, adhering to relevant local force policies and following advice from the **National Cyber Security Centre**
- using a social media management platform for access controls and auditability
- using complex and unique passwords, or passkeys, and securely storing these
- using two-factor authentication (2FA)
- enabling login alerts
- only retaining or approving critically necessary third-party apps
- limits on the use of personal email addresses and devices for business use – any use of personal email addresses will also be required to follow security best practice
- where off-network or non-network force devices are used, no accounts should remain logged in, nor should any password or 2FA information be stored on them
- logging out from unknown or redundant devices
- robust processes for managing movers and leavers, noting the associated risk of those leaving as a result of PSD investigations

This list is not exhaustive.

Social media policy

Chief officers should ensure their organisation has a dedicated social media policy, which should set out:

- compliant and ethical use of social media, including general good practice for both personal and professional use
- references to approved accounts and to account owners and administrators
- roles and responsibilities across business areas and operating procedures
- governance processes for the creation and closure of new and old social media accounts, as well as management of any personal and/or sensitive data
- the agreed parameters for the use of off-network or non-network or personal devices in the everyday management of accounts, for content creation and activation of business continuity plans
- the community management procedures for hiding and deleting comments, and for blocking profiles and accounts
- how relevant content, such as public appeals, will be removed or archived in a timely way
- the standards of security and cyber hygiene for force accounts and approved apps, software and hardware
- how breaches of policy will be managed
- business continuity plans in case major social media platforms become unavailable
- clear delineation between social media used for contact and public engagement, and the use of social media accounts for investigations
- related local and national policy, local force guidance

An example of guidance could be a playbook. This is a comprehensive guidebook and living document that outlines an organisation’s social media strategy. This serves as a framework for teams to consistently execute content, engagement and other social media activities, aligned with overall strategy.

For further information go to the NPCC policy guidance on instant messaging and social media (Knowledge Hub login required).

Management of information

Management of social media data should be conducted in line with the **Management of police information APP**.

Tags

APP