

Lincolnshire Police

Policy Document



Social media policy PD174

Policy document information

Reference number:	PD174
Policy sponsor:	Chief Constable
Policy owner:	Head of Corporate Communications
Author:	News and Digital Manager
Publication date:	June 2026
Review date:	June 2028

Version history

Version	Date	Reason for issue
7	March 2019	Biennial Review.
8	February 2021	Biennial Review.
9	May 2022	Complete Review.
10	June 2023	Addition of Accessibility (2.3.7.8) and temporary periods away from work (2.3.15.4).
11	June 2024	Biennial review Access details for the new TikTok account added (2.3.3.6) References to Hootsuite replaced by Orlo. Orlo replaced Hootsuite as our social media management platform in June 2024.
12	June 2026	Biennial review

Code of Ethics

All staff involved in carrying out functions under this policy and associated procedures and appendices will do so in accordance with the principles of the Code of Ethics. The aim of the Code of Ethics is to support each member of the policing profession to deliver the highest professional standards in their service to the public.

Legislative compliance

This document has been drafted to comply with the principles of the Human Rights Act. Proportionality has been identified as the key to Human Rights compliance, this means striking a fair balance between the rights of the staff and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used.

Equality and Diversity issues have also been considered to ensure compliance with the Equality Act 2010 and meet our legal obligation in relation to the equality duty. In addition, Data Protection, Freedom of Information and Health and Safety Issues have been considered. Adherence to this policy or procedure will therefore ensure compliance with all relevant legislation and internal policies.

Other legislation/law which this policy has been drafted to comply with:

- [Human Rights Act 1998 \(in particular A.14 – Prohibition of discrimination\)](#)
- [Equality Act 2010](#)
- [Crime and Disorder Act 1998](#)
- [H&S legislation](#)
- [Data Protection Act 2018](#)
- [Freedom Of Information Act 2000](#)

Security classification

Policy to be published on Intranet: Yes

Policy to be published on Force Website: Yes

Authorised Professional Practice (APP)

This policy has been checked against APP. Since the last review, a specific section has been added to the APP on social media:

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](#).

1. Policy aims (Purpose)

- 1.1. This policy aims to give staff sufficient freedom to effectively use Lincolnshire Police social media accounts for the benefit of public engagement and to support policing activity, whilst maintaining safe and secure working practices.
- 1.2. The policy aims to protect staff and the organisation from the risks associated with running social media accounts, whether on behalf of the force or in a personal capacity, and has therefore been developed with consideration for:
 - Staff security
 - Account security
 - Reputation management
 - Legal risks

2. Policy statement (Key information)

2.1. Purpose of social media

- 2.1.1. The force's use of social media should be built on our communities' needs and best practice guidelines for successfully using social media, rather than the structure of the force.
- 2.1.2. Social media users with no knowledge of policing or its geographic, departmental or functional boundaries should be able to easily engage and benefit from their interactions. Digital engagement should be available to all communities.
- 2.1.3. Police account users should understand who their followers are, their interests and concerns. They should be able to demonstrate meaningful engagement about policing, community safety and local issues. There should be clear responsibility and ownership for accounts and their content.
- 2.1.4. There should be five main purposes for any social media activity (not hierarchical):
- To achieve a tactical, operational policing objective
 - To develop and maintain interest and trust in policing and Lincolnshire Police
 - To change or influence the behaviour of communities to reduce crime and protect community members
 - To enhance and protects the force's reputation and professionalism
 - To obtain the opinions and views of communities about the issues that concern or affect them.
- 2.1.5. To achieve this all our social media accounts should have a clear role and form part of a coherent approach and strategy. There should be clarity of purpose, function and the desired outcomes for each account in line with the above. Each account should have defined objectives and a clear plan for content.

- 2.1.6. Our social media approach should be based on how the public use social media rather than who is responsible for the delivery within the force. Having a high number of accounts presents a risk from both an information management perspective and a lack of clarity to the public and limits the force's ability to consistently engage, with quality content.

2.2. Definitions and types of social media account

- 2.2.1. For the purposes of this policy and the Force's social media operations, social media accounts are categorised as either:

- Official Force accounts
- Personal accounts

2.2.2. Official Force accounts

- 2.2.2.1. Official Force accounts are defined as one assigned to a team, department or member of staff acting in their capacity of an employee or department of Lincolnshire Police to post, communicate and engage with the public.

- 2.2.2.2. A social media account is classed as an Official Force account if it meets one or more of the following criteria:

- The account contains Lincolnshire Police branding, logo or crest in the profile picture or banner image.
- The profile picture is of an officer, PCSO, member of police staff or volunteer that can be identified as a Lincolnshire Police employee such as in Lincolnshire Police uniform.
- The biography or username identifies an association with Lincolnshire Police. For a staff member this could be stating their rank or role and that they work for the Force.
- Most of the content relates to the role or function that an individual or team performs at Lincolnshire Police.

- 2.2.2.3. Official Force accounts are further categorised as follows:

- Corporate accounts (Tier 1)

- Neighbourhood accounts (Tier 2)
- Professional Individual accounts (Tier 3)
- Specialist Team accounts (Tier 4)

Corporate accounts (Tier 1) are the Force's main, top-level accounts that represent the official view or comment from Lincolnshire Police. There is one Corporate account for each social media platform and they are managed primarily by the Corporate Communications Team on behalf of the Chief Constable and Lincolnshire Police as a corporate entity.

Neighbourhood accounts (Tier 2) cover a geographical area in the Force boundary. They are run mainly, but not exclusively, by neighbourhood policing teams and the content should, in the main, relate specifically to the local area they cover.

Professional Individual accounts (Tier 3) are assigned to a staff member who clearly identifies themselves as working or volunteering for Lincolnshire Police and posts and engages in a professional capacity in their specific role. Staff must apply to set up a Professional Individual account, the process for which is outlined in Section 2.3.2. These accounts, whilst owned by the staff member, fall under the governance of Lincolnshire Police, and therefore should adhere to the Official Force Social Media Account Standards as outlined in Section 2.3.6. Professional Individual accounts are different to Personal Individual accounts – a definition for which is described below in Section 2.2.3.

Specialist Team accounts (Tier 4) represent a specific specialist department or team in Lincolnshire Police that has a strong public interest, run by members of those departments. Teams must apply to set up a Specialist Team account, the process for which is outlined in Section 2.3.2. These accounts fall under the governance of Lincolnshire Police, and therefore should adhere to the Official Force Social Media Account Standards as outlined in Section 2.3.6.

2.2.3. Personal Individual accounts

- 2.2.3.1. Personal Individual accounts are those owned by staff in a completely personal capacity and do not identify themselves as working for Lincolnshire Police. Accounts are controlled solely by the staff member and all content posted from them is that person's responsibility.
- 2.2.3.2. However, staff must use their Personal Individual accounts within the confines of other codes and regulations such as the Code of Ethics and Standards of Professional Behaviour, which apply to police officers and staff.

See more on Personal Individual accounts in Section 2.5.

2.3. Official Force accounts

2.3.1. Our social media estate

- 2.3.1.1. The Corporate Communications Team maintains an up-to-date list of all Official Force social media accounts. They are listed on the Force website to give the public a point of reference to check that the account they are interacting with is an official police account. [See list of social media accounts on the force website.](#)

Corporate accounts

The force has eight Corporate social media accounts it can use:

- Facebook www.facebook.com/lincspolice
- Lincolnshire Alert [Home Page - Lincolnshire Alert](#)
- Tik Tok tiktok.com/@lincspolice
- You Tube www.youtube.com/c/lincolnshirepolice
- LinkedIn www.linkedin.com/company/lincspolice/
- X www.twitter.com/lincspolice
- Instagram www.instagram.com/lincspolice
- Nextdoor www.nextdoor.co.uk

Neighbourhood accounts

Neighbourhood accounts are split into fourteen geographical areas.

Lincoln & West Lindsey	East Lindsey	Boston & South Holland	North & South Kesteven
• Lincoln • Gainsborough • Nettleham • Market Rasen and Caistor	• Skegness • Alford and Mablethorpe • Louth • Wolds South	• Boston • South Holland	• Stamford • Grantham • Sleaford • North Hykeham and Bracebridge Heath

Each of these areas has a Facebook Page.

[A full list of Force accounts can be found on our external website](#)

Specialist Team accounts

[See a full list of Specialist Team accounts on the force website.](#)

2.3.2. Requesting a new Official Force account

- 2.3.2.1. It is important that the Force has management and oversight of all social media accounts acting on its behalf. New Official Force accounts should not be created without prior approval from the Corporate Communications Team.
- 2.3.2.2. Running a social media account is resource-intensive, especially when starting a new account. It can take years to build up a significant following and this can only be achieved if users post daily, post interesting content that is relevant to the public, and reply and engage with members of the public.
- 2.3.2.3. The Force must be satisfied that there is a clear, demonstrable public and business need for the account which cannot be achieved or delivered through existing channels and be satisfied that the staff member or Team is committed to running it effectively against our [social media standards](#).

- 2.3.2.4. Staff who wish to create a new Official Force Personal Individual or Specialist Team account must apply by following the request process as outlined below.

Applying for Corporate and Neighbourhood accounts

Corporate accounts are managed by the Corporate Communications Team. Only the Corporate Communications Team can create new Corporate accounts.

The Force Neighbourhood social media estate is managed by the Corporate Communications Team and agreed by the Head of Local Policing. New Neighbourhood accounts (or a reconfiguration of them) cannot be applied for however suggestions can be made by contacting the Corporate Communications Team.

Applying for Specialist Team accounts

Staff can request a new Specialist Team social media account by applying via the Social Media Account Request Form (P802).

Applications require approval from the line manager or head of department. The form then goes to the Corporate Communications Team for consideration.

Staff applying will need to describe the purpose of the account, who the target audience is, what type of content they will publish and who will contribute to it.

They will need to demonstrate that:

- there is a business need for the account and that it offers value to the Force.
- the account will offer a unique insight into policing or Lincolnshire Police or a specific role or department that no other existing Official Force account offers.
- the account will have a clear target audience in the local community and focusses its content to them.

- they are committed to posting regularly and engaging with members of the public including checking DMs and private messages, against our [social media standards](#).

The Corporate Communications Team will consider the application and inform the applicant(s) of the decision.

If rejected, the applicant will be given reasons for the decision. If appropriate, they may be offered access to an alternative existing Official Force account, if one has been identified as offering the same or similar service.

If approved, the Corporate Communications Team will assist the applicant in creating the account to ensure that the appropriate branding and security is set up.

For Specialist Team accounts, an Account Champion should be assigned so that the Corporate Communications Team has a named Single Point of Contact should any issues arise with the account or posts.

Specialist Team accounts will be plugged into the social media management platform (Orlo) but can be accessed via the native platforms. Professional Individual accounts are not plugged into Orlo.

2.3.2.5. If an account is identified as not having gone through the application process, then the account owner will be contacted, asked to suspend the account, and advised to apply for the account through the proper process.

2.3.2.6. Transferees who had an account in their previous force and who wish to continue using it in Lincolnshire, must request to do so via the application process to be considered by the Corporate Communications Team.

2.3.3. Requesting access to an existing Official Force account

2.3.3.1. It is important that the Force has an oversight of who has access to Official Force accounts. Therefore, access must be requested through the Corporate Communications Team so that the appropriate administration and training can be provided.

2.3.3.2. Access to Corporate accounts

Access is reserved only for members of the Corporate Communications Team.

2.3.3.3. Access to Neighbourhood accounts

Staff can request access to a Neighbourhood account by completing the Social Media Account Access Request form (P801). Staff will need their line manager's approval.

If approved the Corporate Communications Team will create a Orlo account for the staff member, through which they will access the account. They will receive an email inviting them to create an account. When doing so, they should also ensure that they set appropriate security on the account, including only using a lincs.police.uk email address and setting a strong password per the guidance in section 2.3.5.

Staff must not share their login details with anyone else or allow anyone else to use their account.

2.3.3.4. Access to Specialist Team accounts

Staff can request access to a Neighbourhood account by completing the Social Media Account Access Request form (P801). Staff will need the approval of the account owner and their line manager (if different).

Specialist Team accounts are accessed through the native platforms.

For Facebook Pages, the Corporate Communications Team will create an account via Facebook Business Manager and give them editor permissions via their own Facebook profile.

Staff can access Specialist Team accounts via a non-work-issued device as the Facebook app is not installed on work devices, but they must ensure they have appropriate security set on their device.

2.3.3.5. Access to Nextdoor accounts

We have retained NextDoor accounts. The county-wide account can be used in exceptional circumstances, but otherwise we will not use NextDoor.

2.3.3.6 Access to TikTok

TikTok is one of the most popular social media platforms and one of the best for youth engagement. However, there are ongoing security concerns regarding TikTok and its use of data and

To mitigate this the following security and access measures are in place for our TikTok account:

- A standalone phone that provides internet access and sim card is used
- The Wi-Fi function on the phone is switched off in its entirety to ensure the phone cannot search for any available Wi-Fi networks at any time
- The phone does not have any force-related apps downloaded to it
- The phone is not used to log in to any force systems
- The phone is not to be connected at any point to any force data provisions, including Wi-Fi
- A standalone Google account is used to for the set up and administration of the account.
- The phone is not used for any other purpose other than for TikTok content gathering and content creation

Only members of the Corporate Communications Team have access to the phone. The account is plugged into Orlo, but only as a back up measure. Posting and content creation should always be done via the dedicated phone.

2.3.3.7 Access to Lincolnshire Alert

Lincolnshire Alert has wider functionality than most social media platforms, as it includes demographic data and survey data. This means it may be of use to people in a wide range of roles across the force, from Neighbourhood policing to Strategic Development.

This means that an account can be requested by any individual in the organisation who has a valid policing purpose to do so.

Accounts will be created by the Public Engagement team, within the corporate comms team. Depending on the role of the requester, different levels of access will be given. The level of access influences the functionality they have access to, but also the geographic area they can see and broadcast to.

Every action on Lincs Alert is fully auditable to the individual.

2.3.4. Social Media Management Platform

- 2.3.4.1. The Force has a social media management platform (Orlo) in place to manage social media access and operations for all Corporate and Neighbourhood accounts. This does not include Lincs Alert, which does not share functionality.
- 2.3.4.2. The Corporate Communications Team retains passwords for all Official Force Corporate and Neighbourhood social media accounts. Only members of the Corporate Communications Team can access the accounts directly through the native platforms, but this is kept to a minimum, for example in an emergency (if Orlo is down or inaccessible) or to amended account information or branding.
- 2.3.4.3. All staff who use Corporate and Neighbourhood accounts must only access them via Orlo.
- 2.3.4.4. Using a Social Media Management Platform provides the Force with the following benefits:
 - **Account protection:** reduces the risk of unauthorised access or hacking and keeps the account as secure as possible by removing the need for users to share passwords. Passwords are retained by the Corporate Communications Team and are accessible to as few people as possible. For Facebook, it removes the need for staff to use their own Facebook Profiles to access a team Page. It also

allows access to be gained only via work-issued devices, which offers a greater level of security.

- **Governance:** offers the Force oversight all Official Force accounts in one place. It allows the Corporate Communications Team to see what is going out locally, monitor account performance and identify opportunities for additional training.
- **Protects the organisation:** allows the Force (via the Corporate Communications Team) to quickly remove any post in the event of it being deemed inappropriate, insensitive, offensive or anything that may cause reputational damage.
- **Protects the staff:** staff have their own username and password to Orlo, which means no one else can ever post as them. It also removes the risk of accidentally posting personal content to a Force account.
- **Accountability:** because each user has their own account the author of each post can always be identified.
- **Auditing:** the platform captures all inbound and outbound messages and retains them even when deleted within the social media platform itself, allowing data to be submitted as evidence or scrutinised by outside bodies such as HMICFRS if ever required, just as a 999 or 101 call would be.
- **Device security:** access can be directed solely via work-issued devices which offers greater security. It means that access via personal devices, which may have little or no security settings set, can be prohibited.
- **Analytics:** social media management tools capture activity from every account plugged into it, giving the Corporate Communications Team the ability to analyse account performance and engagement which in turn aids governance, best practice and evaluation of social media activity effectiveness.
- **Scheduling and post expiry:** staff can schedule pre-written posts. This is useful if they are due to go off shift or on leave or if they wish to post at a certain date/time or at known high-traffic periods.

The platform provides a calendar view of posts so users can see what else is scheduled to go out from the force. It also allows the Force to trigger a lockdown which stops any scheduled messages being published should there be a major operational need. There is also the function to schedule posts to expire, which is useful for wanted or missing persons appeals.

- **Asset management:** allows the sharing of social media materials such as graphics and videos via its content library.

2.3.4.5. The Force recognises that a social media management platform can be limited in terms of its functions and features compared with the native platforms, but it is necessary to have it in place because of the points outlined above. The additional security that a platform offers in itself makes it a vital tool to manage our social media estate.

2.3.4.6. Specialist Team accounts must be plugged in to Orlo, but staff can access via the native platforms.

2.3.4.7. Professional Individual accounts are not plugged in to Orlo and are not accessed through it. Staff can access via the native platforms providing the account and device has suitable security (see 2.3.5).

2.3.5. Account security

2.3.5.1. It is vitally important to minimise the risk of unauthorised access or hacking to an Official Force social media account to ensure that the organisation's reputation is maintained.

2.3.5.2. Therefore, all Official Force accounts (unless stated) should adhere to the access and security instructions as outlined below:

- **Access should be via the social media management platform (Orlo) only for Corporate and Neighbourhood accounts.** Staff have their own log in details to the social media management platform and are given access only to the accounts they need. Owners of Specialist Team and Professional Individual accounts can access via the native app.

- **Accounts should only be accessed via work-issued devices for Corporate and Neighbourhood accounts.** Work-issued devices offer greater security than personal devices. Accessing an Official Force account from a personal device is prohibited. Owners of Specialist Team and Professional Individual accounts, and those using Force Nextdoor accounts can access via their own personal devices but must make sure that their device has suitable security enabled on them (PIN or fingerprint).
- **Two-step authentication should be applied.** Two-step authentication is an extra layer of security. As well as a password, accounts will also need to enter another form of security, such as a verification code sent to a mobile number or email address.
- **Accounts should be registered to a lincs.police.uk email address.** This is so that should there be any issues with the account, for example a requirement to reset the password, that this can be accessed via a Force email address.
- **Accounts should have a strong password.** Strong passwords should be memorable but nearly impossible for someone else to guess. Passwords should be at least eight characters long and not contain any personal information such as a date of birth or pet's name. The National Cyber Security Centre recommends setting passwords using the '[three random words](#)' technique.
- **No access for third-party apps.** Third party apps should not be granted access to an account, except for Orlo.

2.3.6. Social media account standards

- 2.3.6.1. It is important for all Official Force accounts to be standardised in terms of branding and account information, not only to present a professional and consistent look and feel, but to provide the public with the trust and confidence that they are engaging with a genuine, official Lincolnshire Police account.

- 2.3.6.2. Anonymous accounts are not permitted. All Professional Individual Official Force accounts must be clearly identifiable as a real person and must include the staff member's name, picture and rank/job title.
- 2.3.6.3. All Official Force accounts must adhere to these social media account branding standards.

Account name and username

Username and account names should follow a consistent naming convention as follows:

- **Neighbourhood accounts (Tier 2):**
 - **Username:** geographical location suffixed with the word Police, Pol or PoliceUK i.e. @HykehamBHPolice, @HorncastlePol, @LincolnPoliceUK.
 - **Name:** Full neighbourhood policing area name i.e. Bracebridge Heath and Hykeham Police
- **Professional Individual accounts (Tier 3):**
 - **Username:** use your full name i.e @JoeBloggs. Add Lincs or LP suffix if needed i.e. @JoeBloggsLincs or @JoeBloggsLP. Capitalise first letter of names. Do not use ranks in username to avoid having to alter it if role changes or promoted. Rank can be included in the Name.
 - **Name:** Full rank and name i.e. PC Joe Bloggs
- **Specialist Team accounts (Tier 4):**
 - **Username:** @Lincs(TeamName) i.e @LincsRoadsPolicing or @LP(TeamName)
 - **Name:** Lincolnshire Police (Full department name) i.e. Lincolnshire Police Wildlife Crime department

Header banner image

All Official Force accounts should use a corporate Lincolnshire Police banner image provided by the Corporate Communications Team.

Profile picture

The profile picture should be a clear, high-quality photo as follows:

- **Corporate (Tier 1) and Neighbourhood (Tier 2) accounts:**
Official Lincolnshire Police crest.
- **Professional Individual accounts (Tier 3):** High-quality head and shoulders picture of staff member in uniform or work attire.
- **Specialist Team accounts (Tier 4):** Official Lincolnshire Police crest or high-quality photo of team or related image.

Biography

The biography should contain details of the role or area covered by the account and details on how to report crime. It should follow the appropriate template as below:

- **Corporate (Tier 1) and Neighbourhood (Tier 2) accounts:**
 - **Twitter:** 'This account is not monitored daily. Do not report incidents here. Report crime or make complaints on our website or call 101. Call 999 for emergencies only.'
 - **Facebook and Nextdoor:** 'The official neighbourhood policing page for Grantham and surrounding area.
This page is not monitored daily.
Do not report crime here. Dial 101 or report online on our website. Call 999 for emergencies only.
Make complaints on our website at
<https://www.lincs.police.uk/make-a-complaint>
Please be courteous to one another when commenting on our Page. We reserve the right to ban anyone who posts derogatory, offensive or hateful comments.'
- **Professional Individual accounts (Tier 3):** Brief overview of role followed by 'Do not report crime here. Dial 101 or 999 in emergencies only.'
- **Specialist Team accounts (Tier 4):** Brief overview of the role of the department followed by 'Do not report crime here. Dial 101 or 999 in emergencies only.'

Location

- **Corporate accounts (Tier 1):** Full address of Police Headquarters, Nettleham if space allows, or Lincolnshire, UK
- **Neighbourhood (Tier 2):** Full address of main local station if space allows, or main local town i.e. Grantham, Lincolnshire.
- **Professional Individual accounts (Tier 3):** Main location of work or area covered i.e. Skegness, Lincolnshire or East Lindsey, Lincolnshire.
- **Specialist Team accounts (Tier 4):** Main location of work or area covered i.e. Skegness, Lincolnshire or East Lindsey, Lincolnshire.

Website

The related website listed should be www.lincs.police.uk.

2.3.7. Using Official Force accounts

2.3.7.1. Frequency of use

Whilst there are no exact requirements for how often accounts should post, they should be posting regularly enough to keep the account active and engaging. Content should be timely and relevant.

Social media accounts can quickly become flat and stale if left unused and can lose followers, so regular use is vital.

The Corporate Communications Team regularly monitor and assess usage and will contact account owners with advice if an account appears under-used or is not engaging with the public regularly.

If an account is identified as being inactive for an extended period of time, or if account owners can no longer commit to using it regularly, then consideration will be given to closing the account or advising the staff member to convert it to a Personal Individual account where appropriate.

2.3.7.2. Tone of voice

A tone of voice and style of writing is important as different communities relate better to different things.

In the main, staff should adopt an informal tone of voice but should adapt depending on the content being posted. For example, an appeal for information requires a more authoritative tone.

Above all else, staff should remain professional, polite and respectful to followers and authors of inbound messages at all times, just as they would during a conversation over the phone or in the street.

2.3.7.3. Engaging with followers

Social media is a two-way engagement tool. It is social, and there is an expectation amongst communities on social media platforms that accounts engage and not just be used as a one-way broadcasting tool.

It won't be possible, nor necessary or appropriate, to respond to every inbound message, but every effort should be made to check inbound messages daily and respond to them in a timely manner. This is to ensure that any questions and queries are answered, or any information or intelligence can be gathered quickly. Followers don't like to be ignored and will quickly complain or unfollow if they experience this.

If an account cannot commit to this, then consideration must be given to closing the account.

2.3.7.4. Private messaging and Direct messaging (DMs)

Private messaging on social media should never be considered a secure means of communication. Therefore, staff must not engage in private conversations with members of the public where the content includes sharing personal private information or operationally sensitive information. Any such conversations must be moved to other official channels, such as force email, at the first opportunity and any messages containing such information must be deleted immediately from the social media account.

Private messaging on Facebook accounts should be switched off and not be used. This is because the Force does not have the capacity to 24/7 cover of our social media estate to effectively deal with and respond to messages. And because there is a risk of missing a critical report, it is better to not offer this contact method.

2.3.7.5. Content creation

Staff are encouraged to use different forms of media to accompany their posts or look to find new and creative ways to use their account.

Stock images, videos and campaign materials are made available to staff who have access to Orlo, via the platform's content library.

Permission should be sought from all staff and premises that feature prominently in images or videos before posting and the permission documented.

Staff should not take images or videos from Google or other search engines where the creator has not granted copyright-free use. See more on Copyright in section 2.3.14.5.

Full guidance, advice, tips and best practice for creating engaging content is available on the [Social Media section on the Intranet](#) or they can contact the Corporate Communications Team.

2.3.7.6. Following other accounts

Following is considered a sign of endorsement so staff should be mindful of following other accounts that have particularly strong, inappropriate or offensive views or opinions that may conflict with the Force's.

2.3.7.7. Housekeeping

Old content on social media accounts may be left for information purposes, but anything operational must be deleted after six months. All Caught on Camera, Most Wanted and Missing Person appeals can be dealt with solely by Corporate Communications.

2.3.7.8. Accessibility

The Force has a responsibility to make its content as accessible as possible. Accessibility is about ensuring our content can be accessed and understood by the widest possible audience.

It benefits people with visual, hearing, mobility or cognitive impairments, learning difficulties and those who use assistive technologies when using the web.

It can also benefit people who may have other access issues, such as situational (noisy environments), those using mobile devices and smaller screens or have slow internet connections or those who have hardware or software limitations. Good accessibility benefits everyone.

Users of social media accounts should endeavour to make their content as accessible as possible as follows:

- Avoid text in images: Text in images cannot be read by a screen reader and also does not scale up or down very well so may be difficult to read on different screen sizes.
- Add alt-text to images: Alt-text is used to describe an image so that it can be read out to people who are using screen readers (so helps people with visual impairments). It also displays if an image fails to download, therefore assisting those with poor internet connection. Publishing images containing text should also be avoided.
- Add captions on all videos: Not only useful for those with hearing difficulties, but also so those in noisy environments or situations where having sound on is not appropriate.

[Creating accessible digital content](#)

2.3.8. Dealing with reports of crime or incidents

- 2.3.8.1. The Force cannot accept reports of crime on our social media accounts. All Force accounts should state that reports of crime should not be made via the channel and direct members of the public to the [online crime reporting tool on the Force website](#) and 101 or 999 in emergencies. If a member of

the public attempts to report something in this way, they should be replied to as soon as possible and directed to the correct reporting process.

2.3.9. Dealing with intelligence

- 2.3.9.1. Intelligence should not be solicited openly on a social media account as this can put the author or subject(s) of the intelligence at risk.
- 2.3.9.2. Accounts receiving inbound messages which constitute intelligence should ask the author to submit their information through the force's website (by posting the author a link to the website by way of reply) or by calling 101.

2.3.10. Dealing with complaints

- 2.3.10.1. A member of the public making a complaint on an account should be directed to the [complaints page on the Force website](#). The Professional Standards Department receive the complaints submitted.
- 2.3.10.2. Staff should not engage with or try to resolve the complaint by continuing the conversation over social media, unless they are of a low-level nature e.g. 'service recovery'. This is to ensure the details of the complaint remain secure and out of the public domain and are directed through the correct channel to the Professional Standards Department.

2.3.11. Dealing with negative, abusive or offensive comments

- 2.3.11.1. Police social media accounts inevitably attract comments from members of the public which are negative, disparaging, critical or offensive. However, it is important to allow free speech, open discussion and opinion and not stifle criticism, challenge or debate.
- 2.3.11.2. It is also important, where appropriate, to address concerns and criticism addressed by replying in a respectful and professional manner. Where criticism is directed at a high-profile incident, whether local or national, or at a Force position on a particular subject, replies should reflect the force's official position on the matter being debated. Staff should contact the Corporate Communications Team for advice if required.

- 2.3.11.3. Comments that cross the line into using bad language, posting offensive images, inciting any form of crime or disorder, or making any comments or allegations which constitute bullying, a hate crime or defamation/libel should be flagged immediately to the Corporate Communications Team. When reporting the behaviour, staff are advised to capture an image of the offending post as evidence.
- 2.3.11.4. Action will be proportionate to the behaviour but may include blocking the commenter, reporting them to the social media platform they are using, or, in the most serious cases, bringing to the attention of the Force's cyber-crime unit.

Our procedure for comments is:

We reserve the right to remove comments and block you if we feel you offend, intimidate, hurt, or deliberately provoke specific people or groups of people.

We welcome open debate; we welcome free speech that allows you to articulate their opinions without fear of retaliation. But we do not welcome discourse from anyone who does not respect and live by those same principles. We live in a society where freedom of speech is a right, but if you abuse that right you can expect to be sanctioned.

If anything you post tips the balance towards hate speech – this is defined as anything public that expresses hate or encourages violence towards a person or group based on something such as race, religion, age, sex, nationality, ethnicity, disability, or sexual orientation – or that post anything that threatens, incites, or encourages hatred or violence in any way, we may record this as a crime and investigate you in the same way we would as if this had happened on the street.

Be aware of what you post, be mindful of how others may receive it, and, above all, be kind to one another. Thank you.

(If you've been blocked and wish to appeal or complain about the service you have received,

visit <https://www.lincs.police.uk/fo/feedback/complaints/complaints/>)

2.3.12. Dealing with Freedom of Information (FOI) requests

- 2.3.12.1. FOI requests made to an Official Force social media account are considered a legitimate means of contact and must be responded to in the normal way, as long as they contain a valid name, valid address and details of the information requested. In this case, they should be promptly forwarded to the 'FOI inbox.'
- 2.3.12.2. If the FOI request does not have the valid details the requester should be referred to the [FOI pages on the Force website](#) which provides guidance on the submission of such requests. Legislation within the Freedom of Information Act 2000 dictates that once the Force receives the request it has to be responded to within 20 working days. Therefore, a prompt response to the requestor and notification to the Data Protection Team is essential.
- 2.3.12.3. The Data Protection Team can be contacted on Ext 47120, 47122 or 47125 for any queries regarding FOI.

2.3.13. Dealing with media enquiries

- 2.3.13.1. Staff should be mindful that members of the media do monitor Force accounts to search for potential newsworthy items. Therefore, it is worth pausing before posting to think about what impact it might have in the media.
- 2.3.13.2. Highly newsworthy posts may quickly lead to inbound enquiries from journalists direct to a social media account or into the Corporate Communications Team. If a post is likely to generate a high level of interest in the media, whether good or bad, then it is important to contact the Corporate Communications Team beforehand to warn of the potential for a high volume of enquiries and to get professional advice on how to handle the situation.
- 2.3.13.3. Staff should not engage in direct conversations with journalists over social media as this may lead to them being directly quoted without warning from

the journalist. Journalists should be directed to the Corporate Communications Team if they wish to enquire further.

2.3.14. Media law

2.3.14.1. All the Force's social media content is covered by British media law and the same rules apply to Lincolnshire Police as they do to the news media and the general public.

2.3.14.2. Defamation

Defamation occurs when someone makes a false statement about staff or group of staff members which causes reputational damage if published or broadcast.

There are six defences against defamation based on strict criteria and conditions.

In the context of police use of social media, risks include publishing posts which infer or suggest guilt at a point when nothing has been proven in law, publishing comments not heard in open court, publishing information about someone that cannot be proven as true, naming someone at the point of arrest, and sharing defamatory comments from another social media account onto one owned by Lincolnshire Police.

2.3.14.3. Contempt of Court Act

Contempt occurs when something is published or broadcast publicly which creates a substantial risk of serious prejudice to active legal proceedings.

In the context of police use of social media, this means that from the point of arrest onwards, nothing should be published or broadcast which could influence a jury and affect a suspect's right to a fair trial.

Risks include posting detailed information about the circumstances of a crime after someone has been arrested or charged, posting information which infers or implies guilt or blame, posting information about a suspect's previous offences, or posting persona.

2.3.14.4. Children and Young People Act

A breach occurs if a child under the age of 18 years is identified while concerned in legal proceedings either as a victim, defendant or witness, unless a court order has been imposed to lift this protection.

Information regarded as identifying a child includes name, address, school, a still or moving image, or any other information which could be used alongside the above to identify that child.

In the context of police use of social media, risks of a breach include naming an under-18 charged with an offence or appearing at magistrates, youth or Crown courts.

2.3.14.5. Copyright

Copyright protects an individual's creative work and is automatic. It covers creative writing, art, illustrations, photography, video, audio, web content, film and TV recordings and broadcasts, and graphic design.

Breaches occur when any such work is copied, distributed (including on social media), replicated or adapted without the owner's written permission.

Risks for police social media include: taking images or videos from Google or other search engines where the creator has not granted copyright-free use, taking images of stolen goods or of vehicles used in a crime from a manufacturer or retailer's website.

2.3.14.6 Sexual offences

Victims of several sexual offences, including rape, have lifelong anonymity from the point of making an initial report. Their details should never be published, not should information that, coupled with information provided elsewhere, lead to 'jigsaw identification'.

2.3.15. Staff leaving the Force

2.3.15.1 Contributors to Corporate and Neighbourhood accounts

On the day a member of staff leaves, the Corporate Communications Team will disable their Orlo account which will remove access to the Official Force accounts they had permissions for.

2.3.15.2 Contributors to Specialist Team accounts

The Account Champion should inform the Corporate Communications Team when an account contributor leaves or will no longer be using the account.

2.3.15.3 Temporary periods away from work

Should a member of staff be temporarily off work due to maternity or paternity leave, sickness or career break, they should make arrangements as follows:

- For contributors to Neighbourhood and Specialist Team accounts, there should be other members of the team with access to the account, in which case, no action needs to be taken. However, in circumstances where the individual is the only contributor, they should seek an appropriate person to cover the account for the period of absence to ensure that the account continues to be active and monitored. That person will need to request access to the account via the process as outlined in section 2.3.3. Specialist Team accounts should not be left without a contributor or be temporarily 'on holiday'.
- Individual account owners should update their biography to clearly state that they are away from work (and include an estimated return date if possible) and will not be monitored for that period.

2.4. Using WhatsApp or other chat platforms for internal work groups

- 2.4.1. WhatsApp, and any type of direct messaging platform or channel, should in no circumstances be used to coordinate team or departmental chats to communicate police information. This includes the arranging or facilitating of overtime, or arranging the deployment of resources. Such platforms are

not protected by Force IT security measures and can be hacked. Anything classed as police information, regardless of its security classification, should not be posted on such platforms.

2.4.2. WhatsApp is not installed on work-issued devices. However, it can be requested if there is a valid business justification for it. Requests must be approved by the Information Management Unit and the Deputy Chief Constable.

- Do not post any offensive, financial, operationally sensitive or personal information, unless the information is suitable for the public domain, for example missing person appeals etc.
- Exercise good judgment and common sense.
- Be polite, responsible & respectful and consider other people's views and beliefs.
- Be accountable and correct mistakes.
- Not to distribute jokes, GIFs, MEMEs and other inappropriate content.
- When setting a profile image ensure that it is appropriate and respectful.
- Not to use the chat as an outlet for negative comments about employees, the organisation or discuss any work-related complaints and HR issues.
- Your actions and comments on WhatsApp must comply with the expected standards of behaviour for a representative/officer of Lincolnshire Police both on and off duty.
- Ensure that your actions are in keeping with The Code of Ethics.

2.5. Personal Individual Accounts

2.5.1. Staff are entitled to have social media accounts for their own personal use but must adhere to the policies as outlined in this section.

2.5.2. Personal account standards

2.5.2.1. There is a clear distinction as to what an Official Force account is and what a Personal Individual account is as outlined in Section 2.2.

2.5.2.2. This is so that the Force has oversight of all accounts acting on its behalf and to avoid any confusion for members of the public as to which accounts are genuine Official Force accounts.

2.5.2.3. Therefore, a Personal Individual account should not:

- contain Lincolnshire Police branding, logo or crest anywhere on the account profile (unless as part of shared content from official accounts).
- contain a picture of the staff in uniform (officer or staff) in the profile picture or banner header image.
- identify themselves as a police officer or staff member working for Lincolnshire Police in your username, biography or in any in post.
- publish content that is work-related posts that only someone working for Lincolnshire Police would be able to post.
- be used to contact or converse with the public on policing matters. If staff are contacted directly, they should be redirected to an Official Force account or another contact channel.
- use a Lincolnshire Police email address or telephone number to register for an account.

2.5.2.4. Should any of the above apply, it will be considered to have blurred the lines between an Official Force account and a Personal Individual account. Account owners will be advised to remove the relevant branding or information or to cease using it as described above. If appropriate, they will be advised of the process to apply for an Official Force account as outlined in section 2.3.

2.5.2.5. It is acknowledged that it may not be possible for staff to completely avoid being known as a Lincolnshire Police officer or member of staff. For example, friends or members of the public may mention a staff member's role or place of work in a comment.

2.5.3. Account security and privacy

2.5.3.1. Personal Individual account owners should take every care to ensure their accounts are secure to avoid unauthorised access or hacking. This includes:

- Implementing two-step authentication on the accounts.
- Ensuring appropriate security is enabled on devices such as PIN or fingerprint.
- Setting a strong password. The National Cyber Security Centre recommends setting passwords using the '[three random words](#)' technique.

2.5.3.2. When using social media platforms which only allow one profile or account per staff, for example Facebook, where secondary 'fake' profiles breach its terms and conditions, users should only identify as working for Lincolnshire Police if they can set security settings on their personal account to limit information to people they know and who they are comfortable knowing that they work for the police.

2.5.4. Standards of behaviour and personal responsibility

2.5.4.1. Staff are trusted to use social media in a personal capacity if they take appropriate measures to maintain their personal safety and comply with other policies and codes determining their behaviour as members of Lincolnshire Police. This includes the Lincolnshire Police force values, The National Code of Ethics and the Standards of Professional Behaviour.

2.5.4.2. How much someone chooses to share is very much a personal decision, however, working for Lincolnshire Police comes with certain responsibilities. Officers and staff are reminded that their behaviour, both on and off duty, online or in person, is subject to the standards of professional behaviour. Staff need to be aware that they are accountable for any information placed in the public domain, even if it's on a private account. Any behaviour which reflects badly upon the reputation of Lincolnshire Police or undermines the trust and confidence in policing in

general may be considered to be discreditable conduct, and may therefore result in disciplinary proceedings.

2.5.4.3. Professional Standards Department guidance states that account owners should not:

- Make offensive comments about the service provided by Lincolnshire Police.
- Make offensive comments of a discriminatory nature about anyone, whether this is a victim of crime, a colleague, a friend, a stranger etc.
- Openly promote their position within Lincolnshire Police on any dating website, whether this be through text used, or images displayed.
- Use their status as an officer/staff member to seek personal gain or pursue personal campaigns.
- Discuss operational or sensitive matters on privately held social media sites or internet messaging service.
- Use personal social media accounts to carry out searches on persons of interest.
- Post information or images you have accessed in the course of your duties.
- Post images (still or moving) of non-public areas of police premises.
- Geo-locate themselves in any police buildings.

If any of the above comes to the attention of the Force, the staff will be contacted and asked to amend or delete the post or detail. The Professional Standards Department will determine what action follows.

2.5.4.4. In line with APP College of Policing guidance, it is recommended that police officers and police staff avoid posting the following on personal social media profiles:

- Employer details
- Details of job role

- Images of uniform
- Mobile telephone numbers
- Home addresses
- Personal email addresses
- Family members' details
- Hobbies and places frequented
- Details of vehicles
- Sensitive information such as racial and political views
- Images of colleagues without their consent

2.5.4.5. Staff should adhere to the terms and conditions of the platform they are using. On Facebook in particular, staff should only have one account and it must be in their real name. Creating fake, ghost or duplicate accounts is against Facebook's terms and conditions. See point 3.1 of [Facebook Terms and Conditions](#).

2.5.5. Using social media for personal gain or as a business interest

2.5.5.1. If an officer or member of staff has an approved business interest, then they can promote their own products and they must adhere to the [Business Interest and Additional Employment Policy PD23](#) when using their personal social media account.

2.5.5.2 However, staff are not allowed to promote or display products on their social media accounts that are not their own in such a way as to generate commercial gain for themselves or others.

3. Other related documents and appendices

3.1. Please list any relevant documentation here, such as other policies that are linked to this one, guidance documentation and the appendices.

- [Appendix 1: Your responsibilities when using a Force social media account](#)

Related documents

- [Social media guidance on the force intranet](#)

4. Monitoring and review

- 4.1 The Corporate Communications Team will monitor the effectiveness of this policy and report to Command Group as necessary.

This Policy will be formally reviewed every two years and amended where required in the interim period to reflect legislative and organisational change.

5. Who to contact about this policy

- 5.1. This policy is owned by the Corporate Communications Team.

Any enquiries about this policy should be directed to:

Head of Corporate Communications

Tel: 01522 9(7459)

Appendix 1: Your responsibilities when using a Force Social Media Account

Your responsibilities

Post regularly

Try to post regularly and consistently but not too much. Your account should not have long periods of inactivity.

Monitor comments

If you have posted something, particularly an appeal for information, make sure you check regularly afterwards for any comments, as they might contain information about an incident.

Also check general comments as people may contact your account direct to ask a question, make an enquiry or make a complaint. Reply if appropriate. As these posts are public, leaving them unanswered will not inspire confidence from the poster or the wider community.

Keep retweeting and sharing to a minimum

Try to focus on posting original content. The public follow your accounts to see what you've got to say, not other accounts. Too much retweeting might even turn followers away. If you do retweet, ensure it is relevant and appropriate.

Don't share across platforms

Please don't share posts from one platform to another, for example, a YouTube post onto your Facebook page. People don't like to be shifted away from the platform that they have chosen to engage with you on, and may not have, or want to create, an account on the platform you are directing them to.

Only follow appropriate and relevant accounts

Keep the number of accounts you follow to a minimum and only to other police accounts and recognised authorities, charities, community groups and local businesses. Following can be seen as a sign of endorsement so try not to follow staffs as you are not in control of their posts and their view and opinions may conflict with ours.

Using images and photos

Ensure you have correct permissions to use photos or images. Don't use images from Google unless you are sure they are open source. If you are taking your own photo, ensure you have the permission from anyone who is the focus of the photo to use it on social media.

Image accessibility

Avoid publishing pictures with text in it and never use images of text as the sole method of communicating. Always use the post text to convey your message. Text in images is not real text and cannot be read by screen readers, meaning people with visual impairment will not know what is in the image.

Good housekeeping

If you posted an appeal, remember to include an incident or crime reference number in your post. If applicable, be sure to remove the post once the person has been found.

Before you post

It's out there forever

Once you post something on social media you have little control over it. Even deleting the post does not necessarily mean it's truly gone, so think carefully before sending.

Restricted/sensitive information

Don't post restricted or sensitive information, such as details of witnesses, victims or suspects/people in custody. If in doubt, consult your line manager or the Corporate Communications Team.

Use an appropriate tone

Think about the tone of voice on your posts according to the content. In the main, adopt an informal tone of voice but an appeal for information requires a more authoritative tone.

Avoid police jargon

Not everyone is familiar with all the acronyms and abbreviations we have in the police force. It may be difficult not to use them when you are restricted by characters but think about whether it would be understood by someone outside the organisation.

Monitoring

Can you commit to checking the comments and interactions? Social media is another way of striking up a conversation - so if you are not prepared to have the conversation, don't start it. Watch the post for at least 15 minutes after publishing to check comments and interact with people commenting on or sharing your content.

Engagement and interaction

Be professional and respectful

Remember that you are posting on a Lincolnshire Police account and speaking for the force. Speak knowledgeably and confidently. Don't be argumentative. Never post anything that might be offensive to others.

Be personable

Let your followers know they are speaking with a real person – talk in the first person, use pronouns such as ‘us’, ‘we’, ‘I’ and ‘our’. Sign off with your name and/or collar number. Use a conversational style and don’t be afraid to show some personality or humour.

Be proactive

Your posts don’t all have to be appeals and crime-related. Don’t wait until something happens to post.

Be responsive

Social media is a two-way and the public expect to be responded to. Reply as quickly as you can to questions and queries. Hit “like” or reply with a simple “thank you” where appropriate. Don’t be afraid to use emojis but don’t use too many. These are easy ways to improve engagement and shows you are listening so will encourage your online community to keep engaging.

Be creative and visual

Use images and videos in your posts. Media-rich posts reach a far higher number of people than plain-text posts. Think of different and interesting ways to show what you and your team are doing.

Try to post regularly and consistently but not too much. Your account should not have long periods of inactivity.

Admit mistakes and respond to them quickly

Be the first to correct your own mistakes. If you make an error, say so and correct it quickly.

Don't be argumentative

Engaging in arguments and inflammatory debates can tarnish credibility and reputation. If you disagree with people, do so respectfully and objectively. When you see misrepresentations about the force, consider correcting this with fact. No arguments, just correct the record.