Leicestershire Police

Social Media Policy & Procedure

PAPER MARKED

F

Policy Owner:	Digital Engagement Manager
Department Responsible:	Communications & Public Engagement
Chief Officer Approval:	DCC
Date of Next Review:	January 2025

This policy has been reviewed against APP and all relevant procedures.

Moved to APP:	Choose an item.
Rationale:	Choose an item.

This document has been produced in conjunction with the Leicestershire Police Legislative Compliance Pack

Review log

Date	Minor / Major / No change	Section	Author
July 2010	Live		Natalie Proffitt
Nov 2011	No Change		Natalie Proffitt
June 2012	Minor		Natalie Proffitt
June 2013	Minor	All Sections	Natalie Proffitt
June 2014	No change		Shilpa Mistry
Feb 2016	Minor	All Sections	Natalie Proffitt
Sept 2017	Minor	All Sections	Meredith Watts
Feb 2019	Minor	All Sections	Meredith Watts
June 2019	Minor		Natalie Proffitt
October 2019	Minor		Shilpa Mistry
January 2023	Major	All sections	Liam Ross

- ## Statement

The public expect modern organisations to be present and active on social media. People want to, and will, use social media to engage with the police, report crime, share information, give feedback or complete a service.

Our main force accounts are followed by 300,000 people, with many tens of thousands more following our wider force network of accounts channels.

Leicestershire Police uses social media primarily to engage with the public. Partner agencies, other forces, senior police officers and the media are secondary audiences. Social media should not be used primarily to interact with these secondary audiences.

We will use social media to

- improve trust, confidence and satisfaction within our communities
- achieve tactical or operational objectives - generating community intelligence, warning and informing, generating responses to appeals, preventing crime
- positively change and influence the behaviour of our communities

- ## Aims

This policy aims to provide clear guidance regarding usage of social media sites and instant messaging applications for all Leicestershire Police staff. It will:

- ensure members of the public and staff of Leicestershire Police are not adversely affected by use of social media or instant messaging applications
- ensure that the reputation of Leicestershire Police is not compromised by staff use of social media

- ## Scope

This policy applies to all police officers, police staff, agency and bank workers and volunteers of Leicestershire Police. For the purposes of this policy, the term ‘staff’ relates to all of the above-mentioned groups.

This policy is intended to support those who use social media channels and instant messaging applications in a professional capacity to engage and communicate with the public. It also covers staff using social media and instant messaging platforms as an unofficial police presence.

Examples of social media include Facebook, Twitter, Instagram, LinkedIn, YouTube, blogs.

Examples of instant messaging applications are Facebook Messenger, WhatsApp, Instagram DMs.

This policy does not apply to the use of digital platforms for intelligence purposes.

- ## Legal Basis

This policy is underpinned by other force documentation, national guidance as well as legislation, which may provide more in-depth guidelines in certain areas:

Force documentation:

- Leicestershire Police’s Trust & Confidence Strategy

- Leicestershire Police's Public Contact Strategy
- Internet Access and Social Networking Procedure

National guidance:

- College of Policing Communications Guidance (Authorised Professional Practice)
- Op Serene
- Digital Policing 2025
- Code of Ethics & Policing Principles
- Nine national recommendations made regarding police officers' use of WhatsApp messaging system
- NPCC National Contact Management Strategy
- MOPI

Legislation:

- Equality Act
- Copyright Law
- Data Protection Act & GDPR
- Media Law and Contempt of Court Act

Monitoring

Leicestershire Police's social media footprint includes approximately 70 accounts. Accounts are set up and access is managed by the Digital Media Team in the Communications and Public Engagement Directorate. The Digital Media Team manages the main force accounts. Other accounts are managed day to day by wider staff. Accounts are limited and creation of further accounts will only be considered on an exceptional case by case basis.

Leicestershire Police does not officiate personal accounts, with the exception of Chief Officers and NPA Commanders. Personal accounts being used for work purposes e.g. to engage with the public, are in breach of this policy and will be actioned appropriately.

All force channels are managed through the force's social media management platform, Orlo. All force social media users will use Orlo to manage social media, including posting to Facebook and Twitter and responding to comments. Orlo will be available to use on force computer, laptop and work-issued mobile devices only. Orlo will not be accessed on a personal device by any force social media user.

Messages to the force will initially be triaged by the Digital Desk based in CMD, using Orlo's keyword triaging technology. Posts will be assessed based on triggers and other criteria under THRIVE, and actioned if required. This could include an immediate police presence, or creation of an intelligence log or crime report. If messages don't need actioning immediately, messages will be answered by local users to respond to using Orlo.

Everyone who manages social media accounts professionally must complete social media training prior to receiving access. To request training, contact the Digital Media Team. A refresher social media training session will be attended by users every two years. Good practice and CPD will be shared with users regularly in between. This training will cover best practice use of social media, as well as avoidance of copyright and data protection issues, an introduction to media law and the Contempt of Court Act.

Responsibility for force use of social media will sit with the Digital Media Team who will monitor ongoing usage for any issues, feedback and ensuring this policy is put into practice.

Instant messaging apps, such as WhatsApp, can be used by officers to engage with the public in some contexts. Please refer to the Social Media Procedure for further guidance. It is important to note that this does not refer to personal use of WhatsApp, both between groups of colleagues and between staff and individual members of the public. Other associated policies and procedures apply to this such as – Management of Police Information (MOPI), GDPR, Professional Standards and the Code of Ethics.

Leicestershire Police - Social Media Procedure

This procedure lays out how the force Social Media Policy should be followed and provides supporting information across a range of areas.

Any questions in relation to professional use of social media should be directed to the Digital Media Team – digital.media@leics.police.uk

This includes:

- Requesting new social media accounts
- Accessing existing social media accounts
- Booking training / refresher training
- Seeking advice or best practice
- Changing roles where social media access is no longer required

Account usage

Our primary aim of using social media is to improve trust & confidence in the police by communicating with the public. To achieve this, accounts should be updated and monitored as often as possible. All messages should be read, and responded to where appropriate.

The Digital Media team monitor corporate accounts Monday – Friday in working hours. Out of hours, the on-call Media Relations Officer has access to the corporate accounts.

Posts must be appropriate, accurate and adhere to guidance given in the RAG Guidance. Posts which at first may adhere to all relevant guidance may later be deleted due to new information or criminal proceedings being undertaken.

Other force accounts will be regularly monitored by the Digital Media Team. If an account is used inappropriately, the relevant post(s) will be removed, the individual will be contacted and advice will be given. The issue may also be raised with the individual's line manager and/or PSD.

Training

Training should be requested and booked through the Digital Media Team. Access to social media will not be given until training is completed. The training lasts no more than two hours including time for Q&A.

Further advice is always available – either from members of the Digital Media Team, or self-help resources & advice on the Digital Academy

The below must be read before using social media:

4.1.1 Internet Access and Social Networking Procedure

4.1.2 RAG Guidance

Content of social media messages

Users should refer to the RAG Document for guidance on what can & should not be posted on social media. Full training is also given during Social Media Training. The Digital Media Team can always be asked for advice on content of messaging.

Use of Instant Messaging Services

Leicestershire Police understands that many communities in our force area are active users of instant messaging services, and that police use of these platforms can be beneficial. The most obvious example of platforms of this nature is WhatsApp, but others exist. Across the force, WhatsApp is used to good effect to communicate and share messaging quickly with e.g. those in the rural community to improve trust & confidence, where use of other digital platforms isn't as viable or effective.

Use of these systems for policing comes with a number of risks which must be actively considered and managed by users.

- Staff should conduct themselves professionally at all times while using these services to communicate and are liable to professional standards when doing so
- Users should be aware that they could be subject to audit at any time so they should be able to justify their use of social media at any time.
- Instant Messaging services should not be used professionally on personal mobile devices – use work devices only
- Any inappropriate content or conduct witnessed should be acted on appropriately
- Crimes or incidents witnessed should be recorded & acted on appropriately
- More than one member of staff should have access to a group for resilience
- Line managers will have access to WhatsApp group(s) on request
- 1 to 1 messaging with members of the public should be avoided wherever possible – stick to established community groups, or build your own
- Your rules of engagement should be set out clearly to your groups, for example, WhatsApp is not a crime reporting channel but meant for two-way engagement

Users looking to establish or join a Community WhatsApp group should engage with the Digital Media Team who will discuss specific usage and feed this into the LPD Communications and Engagement working group for approval, so it can be logged & audited appropriately.

The IT Department can enable WhatsApp on your work device.

Individual / Personal Accounts

Leicestershire Police understands that staff will use social media in a personal capacity. HR & PSD guidance should apply to those using these platforms during working hours.

For information and guidance on the use of personal social media accounts, please read the Internet Access and Social Networking Procedure

Personal accounts being used for work purposes e.g. to engage with the public, are in breach of this policy and will be actioned appropriately.

Annex 1 – Support and guidance around removing comments and blocking accounts

When to Remove Comments

Sometimes comments posted by members of the public on Facebook need to be removed, whether this is because they breach this policy, our social media guidelines, or are in contempt of court.

Twitter will only allow a person to remove their own content; comments cannot be deleted by admins, however they can be “hidden”.

You can always report comments to the social media platforms themselves.

You may consider removing comments if:

- it could identify a victim, witness or suspect by any means, e.g. name, address, school, place of work, relationship etc.;
- it identifies a serving police officer or member of staff in a manner which affects their personal safety, threatens violence, is grossly derogatory, or is untrue;
- offensive language has been used which has not been automatically deleted by page filters
- it could be perceived as threatening, abusive or hate speech (targeting a protected characteristic – disability, race, faith, gender, sexual orientation);
- it could potentially put the force into contempt of court (creates bias for a judge or jury e.g. discussions of previous convictions or implying guilt).
- it is defamatory or libellous
- it could be classed as spam e.g. website links, promotional content or repeated messages
- it shares sensitive information e.g. regarding an investigation or covert operation

If you have to remove a significant number of comments, consider explaining why, and provide a link to the social media guidelines. Contact the Digital Media Team for further advice.

Blocking Accounts

Blocking a Facebook or a Twitter user is a last resort and reasoning should be logged and recorded. An effort should be made to engage with the user first. Contact the Digital Media Team for advice before taking action. We need to evidence decisions made in the event of a complaint.

When Offensive Content should be Reported as a Crime

Offensive or threatening content on social media should be reported when it falls into these four categories of criminal offence:

- Credible threats to a person’s life, safety, or property;
- Communications targeting specific individuals or protected characteristics, including persistent harassment and ongoing abuse, and hate crime;

- Breach of court orders, e.g. identifying people protected by law;
- Communications which are grossly offensive, indecent, obscene or false.

If any police officer or staff member finds content that they consider to be of this nature on social media, they can report it as a crime, following the normal procedures.

‘Repeat Callers’

Repeat callers are those who message a social media page more often than is necessary.

Users will be flagged as a repeat caller if their contact is too frequent, inappropriate or if they are seen to be abusing the contact method. They will be added to the repeat caller list if there are five or more recorded, inappropriate contacts in the space of one month. They will be given advice and if they continue they will be blocked from the account. This system is currently only in place for the Leicestershire Police Facebook page and the @LeicsPolice Twitter account.

If other social media accounts are having issues with repeat callers, they should try to engage with them in the first instance. They can then be directed to the Leicestershire Police Facebook page or the @LeicsPolice Twitter account.