

Policy



Social Media and Instant Messaging Groups

URN: J-P-122

Version: 1.0
Effective Date: 21/01/2025
Version Date: 21/01/2025
Review Date: 21/01/2026

Host Force: Dorset Police (DP)
Host Policy Unit: DP Legitimacy Team
Policy Owner: Dorset Head of Professional Standards
Policy Author: Dorset Head of Professional Standards

Associated Procedure(s): DOR-Pr-050 Force Social Media Accounts Procedure (Dorset)
 DCP-Pr-025 Force Social Media Accounts Procedure (D&C)
 IAG05 WhatsApp Guidance

1.0 Policy Summary

This document provides clear direction on the professional use of social media and instant messaging groups. It sets out the expected standards of behaviour across our organisations, including the OPCCs for both Force areas, ensuring the integrity of and confidence in the police service.

This document is applicable to all officers, staff, members of the special constables, volunteers, agency staff, BT, and other contractors for our organisations, including OPCCs for both Force areas. They will collectively be referred to as 'officers and staff' throughout this document.

All officers and staff must conduct themselves in accordance with the Standards of Professional Behaviour when using social media and instant messaging groups. This applies to their use of social media both inside and outside of work time.

Applicable to:

Devon & Cornwall Police	☒	Dorset Police	☒
OPCC Devon & Cornwall	☒	OPCC Dorset	☒

Officers	☒	Staff	☒
----------	-------------------------------------	-------	-------------------------------------

2.0 Purpose, Standards and Legal Basis

2.1 Purpose

- 2.1.1 The aim of this policy is to ensure that all officers and staff are fully aware of the required standards that they must adhere to when using social media and instant messaging groups, and the expectation upon them when standards fall below expectations.
- 2.1.2 This policy outlines the standards expected for the professional use of social media and instant messaging groups. Inappropriate or unprofessional use of social media and instant messaging groups significantly undermines the public's trust and confidence in the police service and can result in all officers and staff being the subject of misconduct or criminal proceedings. For matters that relate to unsatisfactory performance / capability, or attendance, these are managed in accordance with the appropriate policy and procedure. Please refer to the [People Portfolio A-Z](#) pages of the intranet for further guidance.
- 2.1.3 This policy will provide guidance on how to reduce the risk of individuals or the organisation being compromised by the unsafe / unprofessional use of social media and instant messaging groups. It is also to protect personal or police information from being disclosed inadvertently.

2.2 Legislation

- 2.2.1 Our organisations are obliged to abide by all relevant legislation and other guidance as appropriate:
- Authorised Professional Practice
 - Equality Act (2010) including Public Sector Equality Duty
 - Code of Ethics
 - Standards of Professional Behaviour
 - Freedom of Information Act (2000)
 - Human Rights Act (1998)
 - Media Act (2024)
 - Media Relations Authorised Professional Practice
 - National Decision Model
 - The Data Protection Act (2018) and UK General Data Protection Regulation (GDPR)
 - The Health and Safety at Work Act (1974)
 - Our Purpose (DCP)
 - Vision, Purpose, and Priorities (DP)
 - Police Conduct Regulations 2024

3.0 Roles and Responsibilities

It is the responsibility of every officer and staff member to adhere to the Standards of Professional Behaviour when using social media and instant messaging groups. This applies to both work and personal use. This also includes a proactive duty to challenge and report any behaviour that is not consistent with these standards.

4.0 Policy Information

4.1 Introduction

- 4.1.1 This policy sets out the expected standards of behaviour for all officers and staff when using social media. This includes instant messaging applications such as WhatsApp and Telegram (list not exhaustive). This policy seeks to ensure that everyone fully understands the requirement to use social media professionally and avoid placing themselves, the public and our organisations at unnecessary risk.
- 4.1.2 The use of social media has grown significantly, and it is widely used by organisations and individuals. It provides excellent means of communication, but this brings with it some significant risks and challenges.
- 4.1.3 For the purposes of this policy, social media is a category of internet applications and sites where people can talk, comment, participate, share, network, and bookmark online.
- 4.1.4 The National Police Chiefs Council states that the safe use of the internet and social media requires an awareness of risks across five areas.
- a. Breach of trust or confidence – Disclosure of information obtained by the police service or partners, about the police service or partners, or about colleagues or the public.
 - b. Unauthorised disclosure of personal data – Breach of Data Protection Legislation.
 - c. Bringing discredit on the police service or its partners.
 - d. Revealing personal information – Increased vulnerability to harassment, corruption, or blackmail.
 - e. Revealing operational material or tactics.
- 4.1.5 This policy will provide direction which should minimise these risks, to our organisations and all officers and staff.
- 4.1.6 Failure to follow this policy may be considered as a breach of the Standards of Professional Behaviour with the potential for criminal and/or misconduct proceedings to be initiated. For matters that relate to unsatisfactory performance / capability, or attendance, these are managed in accordance with the appropriate policy and procedure. Please refer to the People Portfolio A-Z pages of the intranet for further guidance.

4.2 Professional Behaviour

- 4.2.1 Public confidence and trust in the police service can be significantly undermined by officers and staff who use social media unprofessionally. Posting or sending messages that are offensive, derogatory, discriminatory, or insensitive in their

nature, even in instant message groups (e.g., WhatsApp), discredits those involved and the police service in general.

- 4.2.2 In addition to causing reputational damage, this type of behaviour has led to individuals from forces around the country being subject to misconduct and even criminal proceedings. The consequences of this have included the immediate dismissal of officers and staff whose conduct is found to amount to gross misconduct resulting in placement on the Police Barred List. Some have received custodial sentences on conviction for criminal offences due to the abhorrent nature of their social media use.
- 4.2.3 As with all areas of policing, the Standards of Professional Behaviour and the Code of Ethics are fundamental to how officers and staff should always conduct themselves, whether inside or outside of work time. This also applies to the use of personal social media accounts and instant message groups.
- 4.2.4 Officers and staff must demonstrate the high standards of behaviour expected of them when using social media and instant message groups, in the same way that they would in public or in the workplace.
- 4.2.5 There will be no tolerance for any posts, messages or imagery that feature themes of:
- Racism
 - Sexism
 - Misogyny
 - Misandry
 - Homophobia

Or are:

- Obscene or grossly offensive
- Derogatory or offensive about colleagues
- Derogatory or offensive about members of the public
- Bullying, harassing or an abuse of power in nature.

This includes any posts which are discriminatory against the protected characteristics as defined by law.

- 4.2.6 Officers must understand that due to the obligations placed upon them by the Standards of Professional Behaviour their rights to respect for a private and family life under Article 8 ECHR are restricted. This was established by the case of *BC and others v. CC Police Scotland* [2019]

“an officer’s reasonable expectation of privacy is limited because of the attributes of a constable for whom the Standards of Professional Behaviour applies”.

- 4.2.7 Home Office Guidance – Conduct, Efficiency and Effectiveness 2020, states the following:

Particular care must be taken when considering the private online behaviour of a police officer, even where they are not immediately identifiable as such. Consideration of off-duty online activity should take into account the officer's right to privacy and to free speech.

However, the ultimate test is whether that online activity, notwithstanding that it is done in a private capacity, breaches the Standards of Professional Behaviour and brings discredit to the police as a whole. Paragraph 2.19.

It goes on to clarify:

It is important to recognise that any content or messages that are shared with colleagues via social media, email, text message or encrypted messaging services (even in an off-duty or private capacity) are nevertheless shared with workplace colleagues. Due care should, therefore, be taken as any material is potentially reportable. Where shared with other officers or staff, whether an individual is actually off-duty at the time that such a message is sent may not be relevant – individuals should apply the test as to whether the comments, content or material would be considered appropriate in the workplace and in line with the Code of Ethics and Standards of Professional Behaviour before sending or sharing any material in this way. Paragraph 2.20.

- 4.2.8 Although the above quotes (4.2.6 and 4.2.7) from the Home Office Guidance refers to officers, to be explicitly clear, there can be little expectation for privacy by officers and staff when it comes to their use of social media even when it is for personal use or in instant message groups, where messaging is being shared between colleagues.

For example, if you are a member of an instant message group with friends or family, some, or all of whom are also work colleagues, you are governed by the Standards of Professional Behaviour and have a personal responsibility to report inappropriate content authored by a colleague and any responses to that content by colleagues. Examples of groups include:

1. Work related – membership consisting of police officers and police staff only and for the purpose of sharing work related content.

Requirement to challenge and report inappropriate content to first- or second-line manager, as appropriate. Line manager to consider if a referral to PSD is required.

2. Private group – membership with others who are not related to Devon & Cornwall and Dorset Police e.g., family or friends.

No requirement to report, however officers and staff are reminded of the revised Code of Ethics which states you must do the right thing in the right way for the right reasons.

3. Blended private group – membership consisting of non-policing personnel **and** police personnel and for the purpose of sharing non-work-related content e.g., arranging social functions. Will also include positive reactions to content e.g., thumbs up or laughing emoji etc.

Requirement to challenge and report inappropriate content posted or 'reacted' to by a work colleague. Reporting as per point 1-, first- or second-line manager. Line manager to consider if a referral to PSD is required.

This policy is unable to cater for every conceivable situation regarding membership of groups and whether it is deemed work or non-work related, and therefore each case will be reviewed by PSD on a case-by-case basis. However, the principles of the Home Office Guidance will be followed and therefore content, authored by colleagues regardless of the purpose of the instant message group, will be subject of reporting responsibilities should the content fall into any of the categories outlined in 4.2.5.

- 4.2.9 Attempts are often made to dismiss the above types of behaviour as harmless banter. This is not a defence for behaviour which is offensive, malicious, or bullying in nature. What one person may perceive as harmless banter or humour can be deeply offensive to others.
- 4.2.10 Officers and Staff have a positive duty to challenge the conduct of their colleagues. Where necessary, they must challenge and report to their first- or second-line manager, as appropriate, any behaviour that falls short of the expected standards. The line manager to consider if a referral to PSD is required.
- 4.2.11 Failure to respond to any inappropriate conduct by your colleagues that you are aware of is a breach of the Standards of Professional Behaviour and may lead to misconduct proceedings.
- 4.2.12 Officers and staff are responsible for the content of any messages or images that they receive from family and friends, who are also colleagues and will be expected to challenge and report to their first-or second-line manager, where there is a breach of the Standards of Professional.
- 4.2.13 In addition to reporting to a line manager, both organisations have a confidential reporting system Confide in Us, which can be located via the links below.

Confide in Us (DP Link) Confidential Reporting System

Confide in Us (DCP Link) confideinus

- 4.2.14 Wilful blindness or simply leaving an instant message group to distance yourself from the behaviour is not sufficient. Any content that breaches the Standards of

Professional Behaviour must be challenged and reported to a first- or second-line manager, as appropriate. The line manager to consider if a referral to PSD is required. Please refer to 4.2.10.

4.2.15 Using the facility to automatically delete posts or messages after a short period of time, or immediately deleting messages after they have been received, does not negate the offence they may cause. Nor does it prevent disciplinary action being taken. Messages and posts can often be recovered.

4.2.16 Officers and staff must be alert to the potential for instant message groups to be used by colleagues to exploit more vulnerable members of staff and to form inappropriate relationships. Any concerns must be challenged and reported to a first- or second-line manager, as appropriate. The line manager to consider if a referral to PSD is required.

4.3 Disclosure of Police Information

4.3.1 The improper use of social media and instant message groups can lead to sensitive police or personal information being released into the public domain. There can be a wide range of consequences to this including.

- Loss of public confidence in the police service,
- Jeopardising ongoing operations, investigations, or prosecutions,
- Placing individuals at risk of harm,
- Prosecutions under Data Protection legislation,
- Misconduct proceedings.

4.3.2 It is important to remember that whilst some social media platforms offer end-to-end encryption this does not mean that they are secure. Widely used and trusted platforms, including WhatsApp, have been subjected to security breaches in recent years.

4.3.3 Microsoft Teams should be utilised wherever possible for any instant messaging groups within a team or department. Teams is now supported on most mobile phones, as well as PDAs and laptops issued by both Forces.

4.3.4 Information Assurance Guidance IAG05 - Use of WhatsApp by Force Personnel provides specific guidance on using all unsupported instant message tools (including WhatsApp) for work purposes. Anyone using WhatsApp or a similar platform in this way is strongly encouraged to read this guidance. (See Section 6). It will be the responsibility of the Information Asset Owner (Head of Department) to approve closed messages groups such as those used to support on-call rotas and call out groups. When approval is granted, the following is to be recorded in the Asset Register:

1. Name of the group
2. Members of the group
3. Purpose of the group

For guidance on the Asset Register please contact Information Assurance, InformationAssurance@devonandcornwall.pnn.police.uk

- 4.3.5 Where instant message groups are used for work related discussions, they must not be used to share personal, sensitive, or investigative information. If this type of information is shared, it must be risk assessed and done only where there is an urgent requirement, and no other means of communication is available. The use of personal devices in this way should be avoided wherever possible. Where they are used, it is advisable to have an agreement in place to define exactly how the group will be used as outlined in 4.3.4 and processes should be in place to ensure that the groups are decommissioned after their use and appropriate information is transferred to Force systems as soon as possible.

Under Freedom of Information Act (FOIA), information shared via closed messaging groups may be considered disclosable if a request is received. This is not limited just to 'corporate' or 'official' channels and non-corporate or personal messaging groups where messages have a direct, formal connection with the public authority are also potentially subject to FOIA.

If an instant message group is used for the purpose of on-call and/or call outs, when resources are identified all further communication must be via a work device for the purpose of briefing/deployment.

The following are examples of personal, sensitive and investigative information that must never be shared via social media channels or instant messaging groups (list not exhaustive):

- Details of scenes
- Scene photographs
- Images of suspects/victims
- Named parties.
- Addresses
- Details of allegations
- 3rd party contact details
- Any other material that relates to operational activity

- 4.3.6 The Forces Social Media Accounts Procedure DCP-Pr-025 (DCP) and Social Media Accounts Procedure DOR-Pr-050 (Dorset) provides clear guidance on how to set up and use social media accounts to engage with the public on behalf of our organisations. Please refer to the procedure for more information (See Section 6). However, the following must not be disclosed.

- Official information (where handling notes show it is for Police Use only, sensitive, or not for publication).
- Information that could identify (directly or by inference) living persons without a policing purpose unless it is justified, necessary and a lawful basis has been identified to disclose.
- Operationally sensitive information.
- Commercially sensitive information.

- Information that may be subject to copyright or intellectual property rights.
- Any other information that could cause reputational harm to our organisations.

4.4 Security and the Risk of Compromise

- 4.4.1 Officers and staff must be aware of the digital footprint that they leave when using the internet and they must recognise that it can be difficult, and sometimes impossible, to remove information from social media once it has been posted.
- 4.4.2 It is strongly recommended that officers and staff do not put personal information on to their social media accounts. This includes telephone numbers, home or email addresses, or details of their vehicles.
- 4.4.3 Officers and staff must not use their own personal social media accounts for professional purposes. Similarly, professional social media accounts must not be used for personal or business interests.
- 4.4.4 It is important to ensure that privacy settings are set appropriately for social media and other applications. This includes allowing Apps access to the device's location data. It must not be assumed that the default settings provide adequate security.
- 4.4.5 Officers and staff must recognise that they could be targeted by groups or individuals who may try to embarrass, discredit, corrupt or blackmail them using information obtained from personal social media accounts. Officers and staff must be aware of the risk and carefully consider how they use social media and the internet.
- 4.4.6 Officers and staff are subject to differing levels of vetting and must be aware that this process will include a review of a person's social media presence. It is important that all officers and staff recognise that their online presence along with their friends and family they associate with online could have an impact on their vetting. This is particularly important for those in, or who aspire to, covert or sensitive roles.
- 4.4.7 Social media provides opportunities for all officers and staff to pursue business interests online. These must be approached in the same way as normal business interests with authorisation being sought from the Head of PSD, in the respective force, before commencing in a new interest or venture or when the officer or staff initially joins the organisation.
- 4.4.8 When using their personal social media accounts, officers and staff must not.
- Incorporate or display reference to any Devon & Cornwall or Dorset Police corporate branded elements within their personal profile.
 - Incorporate, display, or refer to any rank, role, or name of team within either force or identifiable police acronym within the account name.
 - Use either force's name or a variation of this within their account name.

- Mention personal involvement in any police operation or business.
- Within their bio, mention Devon & Cornwall Police, Dorset Police, or any associated force social media accounts.
- Exception to the above will be where such information is shared on 'Professional Networking Sites' (e.g., LinkedIn or similar) for the purpose of personal and/or professional development. In such cases use of the force name is permitted; in addition, details of rank / grade, length of service and brief overview of role can be referenced.
- Capture, publish, share, or use any material or information relating to the business of either force or obtained in the course of your duties, including but not limited to photographs, confidential or protectively marked information, internal communications, operational matters, or tactics.
- Undermine operational, investigative, or criminal justice processes (e.g., contempt of court).
- Under any circumstances refer to any police operation or investigation.
- Under any circumstances divulge or refer to any sensitive operational tactics (e.g., public order tactics and/or covert police techniques).
- Breach copyright laws (using someone else's content without their permission).
- Make defamatory, discriminatory, or bullying comments.
- (Police Officers & Staff in Politically Restricted Posts) Express or support any political view. Please refer to the procedural guidance for Politically Restricted Posts.
- Undertake any activity that could bring either organisations or wider Police Service into disrepute, damage the reputation of the organisations and/or undermine public confidence in policing.
- Disclose any security clearances or vetting levels of themselves or other police personnel.

5.0 Monitoring and Review

Review and amendments will be coordinated by the Policy Unit.

This policy will be monitored by the Dorset Professional Standards Department. Due to the rapidly developing and changing nature of social media the policy will subject to constant review to ensure that it remains effective.

In addition to this, the policy will be reviewed on at least an annual basis from the date of first publication.

6.0 Associated Documents

Policy and Procedure

- Corporate Communications and Engagement Policies and Procedures (sharepoint.com)

- Information Assurance Guidance IAG05 - Use of WhatsApp by Force personnel
- Professional Standards Document Library (sharepoint.com) (Dorset)
- Professional Standards Document Library (sharepoint.com) (DCP)
- People Portfolio Document Library (sharepoint.com)

SharePoint

- Code of Ethics (DCP)
- Code of Ethics (DP)
- Our Purpose (DCP)
- Vision, Purpose & Priorities (DP)
- Records Management
- UK General Data Protection Regulation / Data Protection Act (2018)
- Standards of Professional Behaviour - Police Officers
- Standards of Professional Behaviour - Police Staff

College of Policing

- ACPO Guidelines on the Safe use of the Internet and social media by Police Officers and Police Staff
- Authorised Professional Practice (APP)
- National Decision Model
- Media relations | College of Policing (APP)

Other

- Freedom of Information Act 2000 (FOIA)
- Human Rights Legislation
- Social Media SharePoint Guidance
- Engaging and Communicating through Social Media - A Guide for Police Officers and Police Staff 2019
- Dorset Police's priorities. | Dorset Police
- Our ethics | Devon & Cornwall Police (devon-cornwall.police.uk)

7.0 Document History

Present Portfolio Holder: Deputy Chief Constable for Dorset
Present Document Owner: Dorset Head of Professional Standards
Present Owning Department: Dorset Head Professional Standards

Below details required for new documents, major amendments (Dorset only) or novel / contentious amendments (Devon & Cornwall only)

Name of Board: n/a
Chief Officer Approving: T/ACC
Date Approved: 20/01/2025

8.0 Version History

Version: 1.0

Date: 21/01/2025
Reason for
Amendments: Initial document
Amended by: Dorset Head of Professional Standards

We welcome any comments or suggestions you wish to share about the content or implementation of this policy. If you would like to make contact to discuss further, please email .Policies@dorset.PNN.police.uk