Social Media Engagement Policy

Abstract

This policy outlines clear standards for the responsible, effective and secure use of social media and online platforms by officers, staff, volunteers, cadets, and contractors, both as an overt engagement tool in the course of their duties and in a personal capacity where such use may reflect upon the organisation.

This policy does not apply to the covert use of social media or online platforms for research, intelligence gathering or surveillance purposes, which are governed by separate legislation, policy and authority.

Policy

1. Introduction

1.1 The Force maintains a 365 day-a-year communications function which is tasked with managing the flow of corporate information between the police, the workforce, partners, the public and the media. Social media is just one channel in our communications toolkit, and a powerful one, when used well.

1.2 Social media and other digital communication platforms are also commonly used for personal purposes outside of the workplace.

1.3 This policy is intended to enable officers, staff, volunteers, cadets, and contractors (hereafter referred to as personnel) to make, considered, appropriate and ethical decisions about the use of social media in the workplace, and the use of social media and online platforms in their personal lives to maintain and enhance public trust and confidence.

1.4 **This policy applies to personnel**:

This policy applies to all personnel and addresses two distinct and separate areas of social media and digital platform use:

Personal use of any online communication channel, network, application, platform or website, where such use may impact upon the individual's role, public confidence, or the reputation of Surrey Police. This use must comply with the Code of Ethics, Standards of Professional Behaviour, Uk GDPR, Data Protection, Media Law and Misconduct regulations.

(Covered in Procedure sections 6-12)

Use of force-owned or force-managed social media and digital communication channels in the course of employment and in the execution of duties on behalf of Surrey Police.

(Covered in Procedure sections 13-26)

1.5 The policy incorporates recommendations from His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) on police integrity and follows best practice and guidance set by the National Police Chiefs' Council (NPCC) Communications Advisory Group and Authorised Professional Practice (APP), including the NPCC's Use of Social Media and Instant Messaging guidance. This will ensure all social media activity conducted by anyone in Force is carried out consistently and for a legitimate purpose in line with the Standards of Professional Behaviour and the Code of Ethics, adheres to national best practice and demonstrates openness and integrity.

2. Scope

2.1 This policy outlines the practices and standards we require personnel to follow when using social media, and online platforms, and the actions taken in respect of breaches of this policy.

3. Policy statement

3.1 The Force expects all personnel to comply with this policy at all times, to:

- Maintain public trust and confidence in Surrey Police by upholding professional standards of behaviour in all social media and online interactions, on or off duty.
- Protect the confidentiality of victims, witnesses, and vulnerable individuals, ensuring their safety, and dignity are not compromised online, on or off duty.
- Safeguard operational integrity, investigations and sensitive policing activities to avoid the accidental disclosure of information, on or off duty.
- Prevent a breach of trust or discredit the force through unethical, insecure or inappropriate use of social and online platforms, on or off duty.
- Act in accordance with prescribed security practices and protocols to protect the force social media accounts and the management of operation and sensitive data.
- Comply with legal and ethical obligations, including the Code of Ethics, Standards of Professional Behaviour, data protection, media law and misconduct regulations.
- Protect the personal security of personnel, colleagues, family members and friends through association.

3.2 There is nothing within this policy that prevents personnel from using or enjoying social media; however, such use must remain consistent with their obligations as employees or office holders of a public body and the standards of conduct expected of them.

3.3 In the event of an apparent conflict with other policy statements, advice should be sought from the Professional Standards Department and the Corporate Communications department in Surrey Police for consultation with relevant departmental leads**.**

Procedure

1. Why does the Force use social media?

The Force uses social media to communicate, engage, and build trust and legitimacy with its audiences - leveraging its reach, immediacy and sharable nature. It is used to:

- Warn, inform, and maintain public safety.
- Encourage the reporting of crime via a number of non-voice methods and using 999 in an emergency.
- Gather information in relation to reports of crime and incidents of concern that have not been reported. This includes, but is not limited to witness appeals, missing people and wanted people).
- Address mis-, dis-, and mal-information, whether being reported directly to us, or on local channels (where there is a policing link). This can also include addressing local media coverage in relation to data or reports of crime).
- Engage with and reassure our communities, building trust and confidence. Updates of this nature include, but are not limited to, addressing community concerns, arrests, charges, convictions, sentencings, location of missing or wanted people, closure orders, dispersal orders, road closures, and sharing information following a police operation).
- Provide updates around crime, key campaigns, and Force news.
- Share crime prevention advice.
- Promote a career with Surrey Police, whether as an officer, staff member, or volunteer.
- Share positive policing stories with our communities.
- Listen to our communities to address their concerns, answer their questions, and clarify any myths.
- Deliver campaigns in innovative ways, encouraging engagement and discussion.
- Maintain transparent and open communication with the public.
- To amplify partner messaging.

2. Exclusions

2.1 This policy covers the use of social media for engagement and communication purposes both in a professional and personal capacity. This policy does not cover the use of social media for the following investigation and intelligence purposes:

- Contact attempts with missing people. Refer to the Missing Persons Policy.
- Contact attempts with wanted persons.

- Community Tension Assessments (CTA) within non-force owned social media spaces and online platforms.
- Online surveillance and online research. Refer to Internet Intelligence and Investigation Policy (Surrey and Sussex) INTERNAL, Internet Intelligence and Investigation Policy (Surrey and Sussex) (1155).EXTERNAL
- Undercover Online (UCOL) usage – Refer to Internal Serious Organised Crime Hub - SEROCU **– INTERNAL ONLY**
- Obtaining information directly from a social media platform or internet service provider (ISP). Refer to RIPCOM Internal Information**. INTERNAL ONLY**

2.2 In support of investigations and intelligence building, any contact made to the Force owned social media accounts can be recorded in police systems as police information and retained in line with Data Protection legislation.

3. Related policies

3.1 The following policies all apply alongside the Social Media Policy, both in a professional and personal capacity.

Policy	Link to
Acceptable Use of Information and IT Systems	Acceptable Use of Information and IT Systems Procedure Surrey and Sussex.docx
Appropriate personal relationships, conflicts of personal interests and behaviours in the workplace	Appropriate Personal Relationships, Conflicts of Personal Interests and Behaviours in the Workplace (Surrey and Sussex) (1207)
Artificial Intelligence Policy	Artificial Intelligence Policy (Surrey and Sussex) (1236)
Code of Ethics	Code of Ethics | College of Policing
College of Policing Authorised Professional Practice (APP) Engagement and Communication	Engagement | College of Policing
Endorsement Policy	Endorsement Policy (Surrey and Sussex) (1203)
Force Issued Electronic Devices Policy Surrey and Sussex	Force Issued Electronic Devices Policy (Surrey and Sussex) (1177)
Information Management Policy	Information Management Policy (Surrey and Sussex) (1187)
Data Protection Policy	Data Protection Policy Surrey and Sussex.docx
Internet Intelligence and Investigation Policy (Surrey and	Internet Intelligence and Investigation Policy (Surrey and Sussex) (1155) EXTERNAL FOI VERSION

Sussex) (1155) EXTERNAL FOI VERSION Internet Intelligence and Investigation Policy (Surrey and Sussex) INTERNAL	Internet Intelligence and Investigation Policy (Surrey and Sussex) INTERNAL
Joint Force Vetting Policy (Surrey and Sussex)	Joint Force Vetting Policy (Surrey and Sussex) (592)
Media Relations & Integrity Policy	Media Engagement Policy
Missing Persons Policy	Missing Persons and Investigation Policy
NPCC (National Police Chiefs' Council) Artificial Intelligence (AI) Strategy	Artificial Intelligence (AI) Strategy
Use of Email Procedure	Use of Email Procedure Surrey and Sussex.docx
Use of Internet Procedures	Use of Internet Procedure Surrey and Sussex.docx
Wanted Persons	Suspect Management Policy (1242)

4. Related guidance

4.1 While the policy sets standards, local guidance is available to aid in the practical processes of administrating social media accounts and undertaking public engagement and communication. Please refer to Appendix 1 for the Force's social media guides.

5. Who does this policy apply to?

5.1 This policy applies to police officers; police staff; police community support officers; special constables; police volunteers; police cadets; contractors, consultants, agencies, and the staff of, who provide services on behalf of the Force.

5.2 This policy applies in both a personal and professional capacity, when on or off duty.

6. Personal use of social media and online platforms

6.1 Personal use of social media for the purpose of this policy relates to any online platform with a public or private communication or messaging capability.

6.2 Personnel must be aware that their personal use of social media must be compatible with Force policies.

6.3 All information shared within this policy for professional use also applies for personal use of social media and online platforms with communication or messaging capabilities.

6.4 When using social media in a personal capacity, personnel must uphold the same standards of behaviour expected of them in a professional capacity to maintain public trust and confidence and not discredit the Force.

6.5 Failure to adhere to the Standards of professional behaviour may result in disciplinary action, including dismissal and placement on the Barred or Advisory Lists.

6.6 Personal communications must not:

- Breach confidentiality by disclosing sensitive information held by the Force contrary to the UK GDPR, Data Protection Act, Official Secrets Act, National Security Act 2023, and force policy.

- Share, refer to or imply knowledge of sensitive operational activities, intelligence, tactics, capabilities or identities. Personnel should use publicly available search engines to research information published externally by the Force and refer to this if asked questions or decline to answer.

- Share links to content, images or videos that a reasonable person would find inappropriate, discriminatory, abusive, offensive, obscene, distressing, derogatory or cause embarrassment.

- Share or engage in any public commentary that could incite violence or hatred.

- Bully, harass, victimise or discriminate against another person.

- Undermine the operational, investigative or criminal justice process both in relation to the Force – this includes, but is not limited to; being in contempt of Court by breaching reporting restrictions.

- Make public comment on any government policy that affects policing activity – local, national, or international – where all UK police forces are apolitical organisations.

- Make defamatory or libellous comments about individuals, organisations or groups.

- Carry out any other activity that could bring the individual, Force, any other force, or policing into disrepute.

6.7 Personnel are reminded that any information shared online, even if in a private or ‘closed’ group could end up within the public domain and therefore caution on what is shared should be exercised at all times.

6.8 Personnel must not make or accept contact from victims, suspects, or witnesses, met through their paid or volunteer duties with the force. This includes, but is not limited to:

- Sending private messages to
- Following accounts or asking another to follow yours
- Accepting or sending friend requests
- Liking, commenting on, sharing content from or to these accounts
- Any other activity that can be classed as engagement with a social media account.

6.9 Any friend or follow requests received from victims, witnesses or suspects should be reported at the earliest opportunity to the Professional Standards Department (PSD) as a notifiable associate. The sender should be blocked to prevent further contact.

6.10 Personnel should also be mindful that content on social media can connect you to the police service, potentially increasing the risk to yourself, family and friends. This could include but is not limited to; being tagged in police content or content that relates to policing, contact and information shared on LinkedIn, following police satire account e.g. UK Cop Humour, commenting on content related to policing.

6.11 It is highly recommended that personal social media security settings are reviewed frequently to maintain privacy and security. Operational Security has further Force guidance and training available which must be adhered to.

6.13 Dating sites

6.13.1 Any dating profiles must not include photos of videos of personnel in uniform, feature policing equipment, or any policing-related background content. You should also consider how you detail your career or employment to avoid exposure and risks such as blackmail, corruption or embarrassment.

6.14 Social media business interests

6.14.1 Any financial gain as a result of personal social media activities must be declared to Vetting as a Business Interest, in accordance with the Joint Force Vetting Policy (Surrey and Sussex) (592).

6.14.2 In recent years there has been an increase in ‘social media influencers’ online, who are often promoting products or services for financial gain. Should a member of personnel be approached by a ‘social media influencer’ they should not

identify themselves as an officer or member of police staff and should speak to Vetting before engaging with them.

6.15 Fundraising

6.15.1 Prior to promoting or advocating for any online fundraising activities on their personal social media, personnel should conduct their own due diligence to ensure the activity is supporting a registered charity. Others may be more inclined to support a charity championed by you where you hold a role of trust and authority.

6.16 LinkedIn profiles

6.16.1 While the Force operates a LinkedIn company page, LinkedIn profiles are categorised as a personal social media account, therefore the guidance found above is relevant in the usage of profiles.

6.16.2 Personnel should be mindful about the level of disclosure of their profession, skills and place of employment, where this could create a risk to your personal safety. It is strongly advised that while you may engage in subjects such as work/family/private life balance, sharing of too much detail could further elevate the risk to you. You should not advertise that you have specialist policing skills, are security vetted or work in sensitive areas of policing such as Serious and Organised Crime or Intelligence.

6.16.3 Personnel should be aware that fake profiles can exists within LinkedIn, as with any other social space. Care should be taken when conversing with another to ensure operational sensitives or tactics are not unwitting disclosed to a third party or threat actor.

7. Prohibited activity

7.1 The following actions are strictly prohibited:

- Employees must not create, produce, or distribute sexually explicit content online (including through platforms such as *OnlyFans* or similar services).
- Employees are not permitted to profit from the creation or distribution of any sexualised content on any platform. Engagement in such activity will be regarded as gross misconduct.
- Soliciting or sending nude or sexually explicit images (commonly referred to as “cyber-flashing”).
- Making threats of physical violence or engaging in abusive behaviour.
- Making prejudicial, discriminatory, or improper comments to or about colleagues.
- Engaging in stalking, harassment, or any other form of intimidating behaviour.
- Engaging in any form of criminal conduct by any individual, including members of the police service.

7.2 **Use of personal accounts as investigative tools**

7.2.1 Personnel are strictly prohibited from using personal social media accounts to conduct research, monitor online activity, or observe the accounts of individuals of interest. Such activity risks blurring the distinction between legitimate overt activity and covert surveillance, giving rise to “status drift” and potential breaches of legal, ethical and professional standards.

7.2.2 Social media platforms are designed to create and suggest connections between users, including through shared locations, contacts or interactions; the use of personal accounts may therefore result in unintended associations, such as being suggested as a “friend” or contact to members of the public. This may compromise investigations by alerting subjects to police interest, expose investigative methods, and place personnel and their families at risk through unwanted contact, intimidation or blackmail.

7.2.3 All online research, monitoring or surveillance activity must be conducted by appropriately trained and authorised practitioners within designated intelligence or digital investigation units, in accordance with relevant legislation, policy and authority.

8. Monitoring use of social media and breaches of policy

8.1 PSD monitors social media in line with Force policies such as the Lawful Business Monitoring Policy, amongst others, and will deal with any breaches in accordance with the professional standards of behaviour.

8.2 Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the force.

9. Reporting breaches

9.1 Any breach of this policy should be reported to line managers, PSD directly, and Corporate Communications and Engagement, or via Anonymous.

10. Endorsement of businesses, product, and services

10.1 Personnel should be familiar with the Force’s Endorsement Policy to prevent any activity or perceived support for a business, service, or product that will or could result in commercial gain or advantage. If you are asked to feature in any offline, digital, or social media content by a business, charity, or not-for-profit organisation, not affiliated with the Force, where your involvement could generate commercial gain. Checks must be made with Corporate Communications and Engagement before your participation.

10.2 If participation occurs before checks with Corporate Communications and Engagement take place, the business, charity or not-for-profit must be informed that consent to feature is withdrawn and request they do not publish the content into the public domain.

11. Monitoring activities in community groups

11.1 This section applies to online groups not administered or owned by Surrey Police or Sussex Police, such as community discussion pages, neighbourhood forums, and buy-and-sell groups hosted on platforms including Facebook (Meta) and similar services.

11.2 The Force recognises the popularity and effectiveness of local public social media groups; however, personnel must not use their personal social media accounts to covertly monitor any open, closed or secret community groups for a policing purpose. This applies on or off duty.

11.3 Covert monitoring, where group administrators and the public are not aware of a policing presence, may breach public expectations of privacy and freedom of expression under the Human Rights Act (HRA) 1998.

11.4 Further, this covert activity, particularly where the monitoring is repeated to build a bigger picture and results in the collection, or recording of information about individuals or groups, may constitute directed surveillance or where communication takes place require Covert Human Intelligence Source (CHIS) authorisation, depending on the intent and method. Breaches of RIPA require the Assistant Chief Constable to write to the Investigatory Powers Commissioner, notifying them of what happened, which may lead to punitive direction and render any information obtained inadmissible in subsequent proceedings.

11.5 Even when a community group is publicly accessible, users may still have a reasonable expectation of privacy, as the group is not established or administered by police, and members would not ordinarily anticipate law enforcement oversight.

11.6 This area presents a complex challenge for law enforcement, balancing public expectations for action against content shared within such groups with the need to uphold lawful surveillance and privacy safeguards.

11.7 Intelligence Units and the Digital Investigations Support Unit (DISU) have trained specialists who can capture relevant information appropriately and advise whether a proposed activity exceeds initial reconnaissance and requires formal surveillance authorisation.

11.8 Tasking members of the public to observe or report on community groups may also engage CHIS considerations.

11.9 Great care must therefore be taken when requesting or receiving such information, particularly where activity amounts to ongoing monitoring and intelligence professionals should both be consulted and tasked to extract information from community groups.

11.10 Guidance should be obtained from Digital Intelligence & Investigations SMEs on compliance with the Regulation of Investigatory Powers Act (RIPA) 2000 and Internet Intelligence and Investigation Policy (Surrey and Sussex) (1155). Please contact the Digital Investigation Support Unit (DISU) for further information (this unit supports both Surrey Police and Sussex Police).

12. Officers in online groups as citizens - status drift

12.1 If personnel are members of community groups in a personal capacity and happen across content that involves criminality, safeguarding concerns, or intelligence, personnel are likely to feel a duty to act to uphold the Code of Ethics and force priorities. In this situation it is unlikely this would constitute a breach of RIPA, the HRA or force policy, and the matter could be recorded or captured, and reported into the force.

12.2 However, personnel must not continue to monitor the individual, topic, or group for a policing purpose once the information has been reported. Even when undertaken with good intentions, any continued or repeated observation risks becoming directed surveillance without the required authorisation. This can undermine evidential integrity and expose both the individual and the Force to legal challenge, particularly where the distinction between personal and professional activity becomes blurred.

12.3 For further advice or clarification, contact the Digital Investigations Support Unit (DISU), RIPCOM, or consult Internet Intelligence and Investigation Policy (Surrey and Sussex) (1155).

12.4 Please note the formal arbiter for determining whether directed surveillance authority is required in any given circumstance is the force authorising officer within RIPCOM.

13. The Force social media estate

13.1 The Force operates a variety of social media accounts. A number represent the organisation at a Force level, others are specific to geographic areas of the county allowing for more locally tailored content. The tables below set out the types of accounts run by the Force.

13.2

Force level accounts (business pages)	Surrey Police Facebook
	Surrey Police Instagram
	Surrey Police LinkedIn
	Surrey Police YouTube and associated Gmail account.
	Surrey Police TikTok (dormant)
	Surrey Police Snapchat (dormant)
	Surrey Police X

13.3

Local level accounts (business pages)	Elmbridge Beat (Surrey Police) Facebook
	Epsom and Ewell Beat (Surrey Police) Facebook

	Guildford Beat (Surrey Police) Facebook
	Mole Valley Beat (Surrey Police) Facebook
	Reigate and Banstead Beat (Surrey Police) Facebook
	Runnymede Beat (Surrey Police) Facebook
	Spelthorne Beat (Surrey Police) Facebook
	Surrey Heath Beat (Surrey Police) Facebook
	Tandridge Beat (Surrey Police) Facebook
	Waverley Beat (Surrey Police) Facebook
	Woking Beat (Surrey Police) Facebook
	Elmbridge Beat (Surrey Police) X
	Epsom and Ewell Beat (Surrey Police) X
	Guildford Beat (Surrey Police) X
	Mole Valley Beat (Surrey Police) X
	Reigate and Banstead Beat (Surrey Police) X
	Runnymede Beat (Surrey Police) X
	Spelthorne Beat (Surrey Police) X
	Surrey Heath Beat (Surrey Police) X
	Tandridge Beat (Surrey Police) X
	Waverley Beat (Surrey Police) X
	Woking Beat (Surrey Police) X

13.4

Specialist team accounts	Surrey Police Cadets X
	Surrey Police LGBT+ X
	Surrey Special Constabulary X
	Roads Policing – Surrey Police – UK X

13.5

Facebook groups	Use of Force and Stop and Search in Surrey

13.6

Individual officer and staff accounts	Not permitted at this time. LinkedIn profiles are categorised as a personal social media accounts, and should follow the guidance set out in Section 6.16.

14. Roles and responsibilities

14.1 The Force operates a shared accountability model for social media. Different areas of the Force take ownership for their role in the use of social media. This reflects the operational reality that different functions have specific expertise and remits. The table below reflects each department's responsibilities.

No.		
1	Corporate Communications and Engagement	• Corporate Communications and Engagement is the business asset owner of Force and local level accounts. • The department owns and will mobilise its business continuity plans in relation to social media in relation to social media engagement. • The department adds new users and removes previous users (taking direction from local accounts) to the SMMP. • The department will ensure new users within Corporate Communications have access to relevant training for using social media. • The department sets up any new accounts, and closes down any accounts, following discussion and agreement with relevant stakeholders. • The department is responsible for providing relevant guidelines for users around style, tone, imagery. • The department will remove any posts that contravene media law or where welfare concerns are raised and ratified by the officer in charge of a case. • The department will input into relevant development, testing, and adopting of new ways

		of working withing the SMMP, alongside FCC and local policing. • The department, following consultation and guidance from FCC, will block users, only where this is appropriate and all other avenues exhausted. • In consultation with FCC, the department will make decisions around turning comments on / off on posts, or restricting who can comment.
2	Force Command Centre (FCC)	• FCC will act as the first point of contact for all digital contact into the Force. • FCC will provide an initial triage of Threat, Harm, and Risk for the public and the Force. • The department will respond to contact-related enquiries and calls for service in line with the Contact Management APP. • FCC will assign non-contact-related enquiries to either Corporate Communications and Engagement or Local Policing teams for response as required. • FCC will maintain accurate training materials for SMMP users in the Force Command Centre. • FCC will input into SMMP development. • FCC will hide any inappropriate comments or those which contravene media law on social media posts, as outlined in this guidance. • FCC will capture any comments that are inappropriate or that contravene media law for evidential purposes.
3	Information Management	• Information Management will set compliant practices for the secure management of data within Force social media accounts and the social media management platform (SMMP), in legacy systems or in the event of closure. • The department will ensure compliant data practices in the event of a social media account closure. • The department will advise SMMP users of any changes to policy or data practises that could

		impact the delivery of our services through social media.
4	Information Security	• The department will set the standard of security required to manage and use the Force's social media accounts, and will subject these to regular review. • The department will make recommendations in relation to security provisions following reviews, learnings or identified improvements. • In the event of a data breach, Information Security will lead in the protecting of data, securing information, and improving systems to prevent reoccurrence.
5	Internet intelligence and Investigation	• Intelligence and DISU managers and supervisors manage force activity with respect of Internet intelligence and Investigation for research gathering purposes including covert use of social media accounts (not covered in this policy). • The team will ensure evidence is recorded and captured from social media in line with policy. • The team will update relevant stakeholders should the process or requirements for capturing evidence on social media to support investigations change. • They will provide guidance to personnel around using social media in a personal and professional capacity so that they do not breach policy.
6	Learning and Development	• Share guidance around the use of social media both from a personal and professional perspective, at pre-employment stage. • Ensure support and guidance is provided to new recruits around their personal usage of social media. • Provide an overview of social media as a form of contact within Force Command Centre, updating and refining to reflect updates from the SMMP. • Explain that there is a dedicated social media role within FCC that staff may undertake later in their role and training will be provided by the FCC when this is required.

7	Local Policing	• Each of the local policing teams will share content, in line with Force guidance, on their local accounts through Orlo (SMMP). • The local team will monitor posts and respond to comments. • They will follow guidance on style, tone, imagery set by the Corporate Communications and Engagement team. • Local policing users will complete SMMP training before using the platform and complete regular refresher training. • Local policing will raise any posts or comments of concern with Corporate Communications and Engagement at the earliest opportunity.
8	Procurement	• Procurement will support and advise in the tender process for social media platforms or services. • The team will support in the procurement of relevant hardware and software for the Force's social media estate.
9	Professional Standards Department	• The Professional Standards Department will monitor social media usage in line with Force policies. • The team will deal with any breaches in accordance with the professional standards of behaviour. • Deliver training as part of the induction programme, which includes social media guidance.

15. Channels and tools

15.1 A number of social media channels, tools and apps are authorised for use by the Force to facilitate public engagement and communication.

15.2 Authorised social media channels are: Facebook and Facebook Messenger, Instagram, LinkedIn, WhatsApp, YouTube, X, TikTok, Snapchat, BlueSky, Threads, Flickr, Pinterest.

15.3 Authorised tools are: Business Tools for Meta (Meta Business Suite, Business Manager, Ads Manager), Orlo (social media management platform), Clip Champ, Canva, Adobe Premier Pro, Adobe Express, Vimeo.

15.4 Not all authorised social media channels will have an active presence. Usage is defined by the Corporate Communications and Engagement Department.

15.5 Not all authorised social media channels and authorised tools will be accessible by all within the Force. Usage is defined by the Corporate Communications and Engagement Department.

16. Retention of police information from social media

16.1 Data retention durations for content shared on social media should be adhered to at all times. The agreed timeframes for the retention of contact can be found in the 'unified published content data retention durations' document.

16.2 All content should be posted through the social media management platform (SMMP) with an expiry date set. If it is not possible to post content through the SMMP, an expiry date should be set retrospectively through the SMMP once published. Exceptions around posting content natively are outlined in Section 18.3.

17. Social media evidence capture

17.1 Evidence gathering from force social media

17.1.1 Personal social media is not to be used for investigation or intelligence purposes, in line with the III policy.

17.1.2 For the gathering of evidence from any social media or internet source not owned or managed by Surrey Police, refer to the Internet Intelligence and Investigation Policy (Surrey and Sussex) (1155).

17.1.3 Any requirements for the Force to capture evidence from social media can be managed by the Force Command Centre (FCC). Those working on non-voice contact within the FCC should copy text from Orlo (SMMP) the relevant system and upload screen shots or screen recordings, following triage.

17.1.4 If the need for a direct capture from social media is required for an investigation, Officers in Charge (OICs) should initially contact and task the joint force Digital Investigations Support Unit (DISU), who will coordinate capture activity with Corporate Communications and Engagement where the content has been posted within corporate administered accounts.

17.1.5 Where a comment is criminal in nature, it is preferential for DISU to capture evidence directly from social media channels, rather than evidence being captured from the force SMMP. If undue delay could impact evidence capture, to preserve the integrity of the investigations, comments may be deleted.

17.1.6 If comments are prejudicial in that they name a suspect, witness or victim's identity which has not been published by police or disclose unsafe information that has not been published by police, these can be deleted to protect the integrity of the case. Should a prejudicial deleted comment also be criminal in nature, evidence can be obtained from the Force SMMP. Contact the Joint Force Digital Investigation Support Unit (DISU) initially. Where possible posts should be hidden not deleted on

corporate accounts to allow for evidential capture by the DISU by unhiding in a controlled method.

17.2 Contact with victims, witnesses and suspects

17.2.1 Where a member of the public has chosen to engage with the Force (for example, by initiating contact through a force social media account), investigators may request that moderators respond and direct the individual to engage through a private message so contact details can be obtained. This enables investigators to establish direct communication.

17.2.2 Where a suspect or wanted person comments on a public appeal where they are the subject, force moderators can respond to the person. Any contact of this nature must be reported to the Officer in Charge (OIC) of the investigation as soon as comments are made.

17.2.3 Initial (or cold) contact with victims, witnesses, suspects or offenders during the course of an investigation via Facebook and LinkedIn will not be facilitated. (see 17.2.5 for advice).

17.2.4 Initial (or cold) contact with victims, witnesses, suspects or offenders during the course of an investigation via X and Instagram can be considered when all other means of contact have been exhausted. This requires Inspector (or above) level authority and responses will be managed by FCC, in line with their policies and processes. Cold contacts are likely to result in messages being places in spam, as the senders are not known to each other, and therefore this method of communication is not recommended and instead consider guidance under 17.2.5.

17.2.5 Where officers need to trace or engage with an individual known only by a social media profile, intelligence teams or the joint force Digital Investigations Support Unit (DISU) may be tasked to research the account and attempt to identify the likely account holder. Alternatively, or in addition, a consideration should be given to a formal legal request for user information which may be submitted directly to the platform by means of approved processes under appropriate legislation such as the Investigatory Powers Act (IPA), Mutual Legal Assistance Process (MLAP), Crime Overseas Production Orders Act (COPA) or UK production orders via RIPCOM.

For further information on how to task DISU and / or Intelligence teams see here: Digital Investigation Support Unit (DISU) - III

18. Access to social media, tools & apps

18.1 Access to social media, where possible, will be through the social media management platform (SMMP) to provide an auditable log of activity. Access to the Force SMMP is managed by Corporate Communications and Engagement, within contractual license provisions. To notify the department of joiners, movers and leavers.

18.2 To access the social media management platform (SMMP), a Force laptop or desktop computer is required. The SMMP can also be accessed on a force mobile device using a mobile browser. The SMMP is not accessible on personal devices.

18.3 Access to native social media is browser or app based. The Corporate Communications and Engagement Team is permitted to access the sites listed below on Force laptops, Force-issue off-network desktop computers, Force mobiles, and Force-issue off-network mobiles. This will only be when the task cannot be completely through the SMMP.

- Social media platforms: Facebook, Instagram, LinkedIn, YouTube, Reddit, WhatsApp, X, Threads, Snap and Bluesky.
- File transfer services: Dropbox and WeTransfer.
- Email services: Gmail.
- Creative software: Edits, Adobe Creative Cloud Suite, Clip Champ.

18.4 Outside of the Corporate Communications and Engagement team, no other users of social media are permitted to access Force accounts natively.

18.5 Outside of the Corporate Communications and Engagement team, no other users of social media are permitted to access Force accounts on personal devices.

18.6 All users with native access to social media will have two factor authentication in place.

18.7 The SMMP is accessible only on Force devices through single sign on (SSO). If business continuity plans are enacted and access to the SMMP is disrupted, native access will be used to manage Force social media until normal service resumes. Native access will mean the management of Force social media accounts from the personal devices of personnel, and Corporate Communications and Engagement's off-network mobiles. This will include:

- Recording and capture of visual material.
- Editing of visual material.
- Publishing of communications.
- Engaging with/responding to the public.
- Performance reporting.

18.8. Great care must be taken when undertaking any native activity. Personnel must ensure that content is not published from personal accounts in error and that personal account activity does not result in the viewing, engagement with, or creation of unintended personal connections with members of the public.

19. Creating purposeful and compliant communications

19.1 Content shared on any of Surrey Police's social media accounts by any users should maintain public trust and confidence in the Force and UK policing.

19.2 Communications will be compliant with the UK legal and regulatory framework for publication of criminal justice outcomes, which requires reporting and the disclosing of information to adhere to a number of acts including, but not limited to, the Contempt of Court Act, the Children and Young Person's Act and the Sexual Offences Act, the UK General Data Protection Regulation (UKGDPR), Data Protection Act, the Freedom of Information Act and Human Rights legislation. Further information on this can be found in Appendix 2.

19.3 All information published on social media will operate within the context established in the Authorised Professional Practice issued by the College of Policing and Surrey Police's A-Z Media Guidelines.

19.4 There are set conditions and restrictions around the release of photographs on social media for CCTV appeals, wanted individuals, defendants, on conviction, and on sentencing. All this information can be found in the Media Engagement Policy and in Appendix 3.

19.5 To ensure our communications remain complaint with data retention policies, all data retention durations for content shared on social media should be adhered to and can be found in the 'unified published content data retention durations' document.

19.6 Content published from official Force social media accounts must be apolitical unless there is an agreed Force position which has been already made public.

19.7 Users must not comment publicly on the health, or deaths, of Heads of State or government ministers from official Force social media accounts. Strict protocols and a coordinated policing response will see the main corporate accounts and/or Chief Officer team acting as outlets and spokespersons for any condolence messages.

19.8 Users should not disclose information relating to specialist tactics, capabilities, and technology, or other sensitive information that could compromise investigations or operations.

19.9 All users of Force social media accounts are expected to act in line with the relevant policies as outlined at the beginning of this policy plus National Police Chiefs' Council (NPCC) guidance around instant messaging and social media.

19.10 Appeals will only be published on official Force social media accounts that are monitored by Contact staff. The traffic light system outlines who has authority to publish what on these channels.

19.11 Authorised users of Force social media should only complete work-related social media activity when on duty. This includes when on shift, on call, or when specifically requested to do so.

20. How we look after our community on social media

20.1 Our primary and local social media accounts are monitored 24/7 by our Force Command Centre.

20.2 We will remove or hide comments if they are offensive in their nature or deemed to violate our social media guidelines. Information around the process and comments that will be removed can be found in the Principles of monitoring social media guidance.

20.3 Surrey Police reserves the right to block individuals who continually (on multiple occasions) violate the specified social media guidelines.

20.4 The final decision to block an account sits with the Corporate Communications team for both the main Surrey Police accounts and the borough accounts. This decision will be made with input from the Silver in the Force Command Centre (FCC) or the Borough Commander.

20.5 Those working in non-voice contact should not block accounts but should flag concerns to the above points of contact and raising to the Silver in the FCC.

20.6 Content will be issued in line with data retention durations.

21. How to request a new social media account or channel

21.1 All requests for new social media channels or accounts must be submitted to the Corporate Communications and Engagement department for review, which should outline rationale, and how this links with the Force strategy.

21.2 Decisions will be made by the Corporate Communications Senior Management Team and in consultation with any relevant stakeholders and business leads.

21.3 Outside of the Corporate Communications department, all users will only access social media via the SMMP.

21.4 All users of Force social media accounts will act in line with the relevant policies as outlined at the beginning of this policy. Failure to do so will result in the removal of access to social media accounts.

22. How to close a social media account

22.1 Requests to close a specific social media account must be submitted to the Corporate Communications department for review and a final decision, which will be made in consultation with relevant business stakeholders and business leads.

22.2 The closure of any account must be proceeded by a data export, to provide an auditable internal log and to support Management of Police Information (MOPI) compliance. This can be undertaken by the account owner or the respective Force's Corporate Communication department.

22.3 Where closure proceeds a data export, the account will be reactivated by Corporate Communications to facilitate this.

23. Visuals of knives

23.1 The Force does not advocate the use of visuals of real knives or weapons on Force social media accounts. This position is supported by studies by Scottish Violence Reduction Unit, in conjunction with the University of Strathclyde, and the London Violence Reduction Unit in conjunction with University College London.

23.2 In circumstances where inclusion of a knife visual is necessary and unavoidable, the knife will be blurred and inclusion kept to a minimum. Authorisation to include a visual of a real knife will be made on a case-by-case basis by a person holding the rank of Chief Inspector/L2 and above.

23.3 Where the Force is required to communicate about changes to the law or knife amnesties, visuals of knives can be incorporated in a way that does not raise fear but provides clear and unambiguous information for the public.

24. Photography and videography on Force premises

24.1 When capturing photography, videography or audio recording in the course of your role within a Force premise, it is the individual's responsibility to mitigate any operationally sensitive information from being recorded.

24.2 If operationally sensitive information is recorded, the photos, video, or audio must be deleted, or sensitive information edited out before the visuals are published to force social media.

24.3 Photography, videography or audio captured on a Force premise for personal use, on personal device, must be immediately deleted if it inadvertently includes any operationally sensitive information. Personnel should ensure back-up copies are also erased from deleted folders or cloud storage.

25. Use of artificial intelligence

25.1 Artificial intelligence (AI) can be used to aid the creation of Force social media communications using software and apps available on force devices. Communications can take the form of copy or creative.

25.2 Where creative or visuals are wholly created using AI to present a fictious, albeit harmless, reality, this must be made clear to the public.

25.3 Where creative or visual design is aided by AI, this does not need to be declared to the public.

25.4 Where AI is used to aid the creation of copy, the output must be reviewed by personnel for accuracy, adherence to guidelines including tone of voice and brand and subject to the same level of scrutiny as a communication where AI is not used. The result should still be a genuine and authenticate output that creates confidence and positive engagement with the Force.

25.5 AI will not be used to alter any visual material that forms part of an appeal, maintaining a visual representation that is an accurate portrayal of fact and events as they occurred.

25.6 Further information on the use of Artificial Intelligence can be found in the Artificial Intelligence Policy (Surrey and Sussex) (1236/2024).

26. Community groups / blogging sites

26.1 Surrey Police runs one community group on Facebook – 'Use of Force & Stop and Search in Surrey'. This group is monitored by Corporate Communications and Engagement. It is used to hold two Q&As a year and to provide updates following scrutiny panels.

26.2 Surrey Police is not affiliated with any community-run social media accounts including any crime-related Facebook Groups or Pages. These accounts are administrated by members of the public who have access to the same public-facing information as any other member of the community. Our content can be shared to those accounts, as can the content from any other sources. The account administrators are responsible for the moderation of comments, application of their own community management standards and ensuring any legal reporting restrictions are not breached.

26.3 Official social media accounts should not, in general, become members of community groups or blogging sites due to the risk posed to the Forces around unseen calls for assistance.

Team Corporate Communications Team