Social Media Policy (Surrey and Sussex) (1086/2021)

Abstract

This policy is intended to enable police officers, Police Community Support Officers, police staff, Special Constables, volunteers (including Cadets), consultants and temporary staff to make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, LinkedIn, Instagram, WhatsApp, Snapchat, in the workplace and in a personal capacity.

Policy

1. Introduction

1.1 This policy is intended to enable police officers, Police Community Support Officers (PCSOs), Special Constables, police staff, volunteers (including Cadets), consultants, and temporary staff to make appropriate decisions about the use of social media both in the workplace, and in a personal capacity to maintain public confidence and legitimacy in policing.

2. Scope

2.1 This policy outlines the standards we require individuals to observe when using social media, and the actions taken in respect of breaches of this policy.

3. Policy Statement

3.1 Surrey Police and Sussex Police (hereafter referred to as the Forces) expect all individuals to comply with this policy at all times to preserve public confidence in the Forces, our services, officers and staff, partners, and policing UK; to protect the privacy and confidentiality of victims of crime, witnesses, the general public and to preserve the legitimate rights of offenders.

3.2 This policy is not intended to restrict or inhibit activities involving social media in accordance with legitimate engagement or operational activities. In the event of conflict with other policy statements advice should be sought from the Corporate Communications department of the respective Force who will, where appropriate, refer any conflict to the Digital Public Contact board.

Procedure

1. Related Policies / Guidance

1.1 This policy must be read in conjunction with the Information Security Policy, Use of Internet Use of Email procedures, Internet Intelligence and Investigation Policy

Regulation of Investigatory Powers Act 2000 (RIPA), General Data Protection Regulation (GDPR), and College of Policing's Authorised Professional Practice Engagement and Communication. Local Force guidance can be found via Corporate Communications.

2. Definitions

2.1 **Social media users** are people who use social media platforms, in particular to publish content.

2.2 **Authorised social media users** are:

• Social media users who have been authorised by the respective Forces' Corporate Communications departments to post and engage on an official Force social media account

• Retrospective authorisation for social media users will be confirmed by the respective Forces' Corporate Communications departments

2.3 **Official social media accounts** are accounts and platforms that have been agreed by Corporate Communications for use by authorised social media users.

2.4 **Social media** is defined as any online technology (public and private) that allows people to publish content (textual, video, graphical, sound), converse and share content online.

2.5 **Social media** covers an almost inexhaustible list, but the main ones for the purposes of this document include:

• general purpose social media platforms, e.g. Facebook, Twitter, Instagram, and Pinterest

• professional networking platforms, e.g. LinkedIn

• video uploading, sharing and viewing websites, e.g. YouTube, Vimeo and TikTok

• messaging applications, e.g. Facebook Messenger, WhatsApp, Snapchat, Telegram

• InTheKnow

• internal communications collaboration platforms, e.g. Skype, Yammer, Facebook Workplace, Basecamp, Trello, Slack

• publishing platforms, e.g. Tumblr and Blogger

• music streaming, e.g. Spotify, Amazon Music and Apple Music

• live video streaming applications, e.g. Facebook Live and Twitch

• discussion forums and chat rooms, e.g. doctors.net and The Student room

• professional presentation and sharing platforms, e.g. Prezzo, Slido and SlideShare

• user reviews – custody suites etc. Trip Advisor, Google Business Review and Facebook Reviews.

3. Types of Social Media Accounts the Forces Use

3.1 Both Forces make use of the following types of official social media account:

Main corporate accounts
Provide highly newsworthy corporate information that have a significant degree of risk and reputational content, and deliver high priority campaigns while providing a high level of customer care and engagement.

Local accounts
Provide a local point for engagement activity, understanding local and hyper-local priorities and updating the public on interventions to resolve them.

Specialist team accounts
Provide insight into the operation and effectiveness in meeting the Forces priorities.

Individual accounts
Provide some key individuals the opportunity to reassure the public on operational and Force policy, participate in open public debate about policing matters and respond to inaccurate and misleading challenges involving the Forces.

3.2 Only **authorised users** are permitted to post material on an official social media channel in the name of and/or on behalf of the Forces. Corporate Communications will keep a record of authorised users for the respective Force.

4. Obtaining an Official Social Media Account

4.1 Official social media accounts are approved and maintained by the respective Force Corporate Communications department.

4.2 The respective Force Corporate Communications will hold all official accounts' details and passwords, including any linked mobile phone numbers, email addresses, and additional authorised social media users. Access information for approved new official Force accounts must be provided to Corporate Communications within a month of creation. Where existing official Force account information is not held by Corporate Communications, this must be provided when requested.

4.3 All applications for new accounts must be submitted through the Social Media Account request form to the respective Force Corporate Communications with the approval of a Chief Inspector, Band 2 or M1 grade.

4.4 Where an account is approved, accounts will be created by the respective Force Corporate Communications and will be subject to a trial period of 6 months with specific, measurable, achievable, relevant, timely (SMART) performance objectives set.

4.5 All new authorised social media users will be directed to existing Force channels initially. New individual / specialist accounts will be considered but the rationale must clearly support the relevant Force priorities and communication objectives.

4.6 Authorised users are expected to maintain an acceptable professional standards record in line with Conduct Regulations.

4.7 Authorised accounts must be associated to a Force-issued email address and a Force-issued mobile phone number. Personal email addresses or phone numbers must not be used.

4.8 Police officers, PCSOs, and Special Constables, should have successfully reached Independent Patrol status at least 6 months prior to point of application.

4.9 Police staff must have successfully passed their probationary period at least 3 months prior to point of application – unless social media access is stipulated within the role description.

4.10 Volunteers, including Special Constables, should have the approval from the respective Force thematic lead.

4.11 Authorised social media access can be granted earlier than dates stipulated in 4.8, 4.9, and 4.10 where there is a Force priority and with the approval of the relevant Corporate Communications department.

5. Accessing and using official accounts

5.1 Both Forces have social media management software in place and where a licence has been provided to the authorised social media user the management software must be used.

5.2 Native access, i.e. direct access to the platform, by authorised social media users is acceptable in some circumstances, however this must have been approved by Corporate Communications in the respective Force.

5.3 Authorised users will be emailed the social media guidance documents which are bespoke to their Force.

6. Using work–related social media

6.1 The Forces recognise the importance of the internet in shaping public thinking about our Forces and UK policing, our police officers and police staff, partner agencies and others.

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

6.3 Work-related social media must only be undertaken when on-duty, “on-duty” can include when on-call, or when specifically requested to.

6.4 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.

6.5 The primary goal for the use of social media is to maintain public confidence in our Forces and UK policing. This will include:

• maintaining public safety;

• preventing and detecting crime;

• promoting the legitimacy of our policing actions and operations;

• supporting our operational need for community intelligence to assist in investigations, to deter criminality and ensure the vulnerable are informed to keep them safe;

• understanding and gaining insight into legitimate public concerns about crime;

• being transparent and open within our legal and operational constraints about investigations and operations;

• attracting and retaining a diverse workforce of staff, officers, transferees, volunteers, and future leaders;

• promoting the good work of our officers and staff in enforcing the law;

• ensuring the public have access to information to keep themselves and others safe;

• ensuring the public have the right to challenge service delivery;

• challenging myth and misinformation about our Forces, services provided, police officers, Special Constables, police staff and operations.

6.6 Accounts that lie dormant without updates for more than 3 months will be required to submit a written rationale to continue the use of the account.

6.7 We recognise the importance of our staff joining in and helping shape industry conversation and direction through interaction on social media.

6.8 You are therefore permitted to interact on (approved) social media websites about industry developments and regulatory issues.

6.9 Redacted

6.10 Before using work-related social media you must:

• have read and understood this policy and the other policies defined in section 1.1;

• have read and understood other Force specific social media related guidance; and

• have sought and gained prior written approval to do so from a Chief Inspector, Band 2 or M1 Grade.

7. Social Media Content

7.1 **Authorised Social Media Users** should ensure that they:

• do not unnecessarily expose specialist capabilities, including tactics, technology, or officer identities, or other sensitive information;

• adhere to the respective Force's social media guidance;

• adhere to the National Police Chiefs' Council (NPCC) Authorised Professional Practice on communicating arrests, charges, and convictions contained within the respective Force's social media guidance;

• do not unnecessarily include content originating from engagement with the public which has no policing purpose

• do not include content from their personal life which does not have a policing purpose;

• refer to the respective Force's style guide.

7.2 Social media appeals, e.g. witness appeals, will only be published on official social media accounts which have more than one contributor; or are monitored by Contact staff. Please refer to your respective Force's traffic light system for guidance on appeal subjects.

7.3 Social media accounts that are not monitored by Contact staff, or that have less than two contributors, are advised not to enable the option to 'allow message requests from everyone'. If direct messages are accepted, and responded to from the account, the option to have email notifications for direct messages must be enabled for audit purposes.

7.4 Social media accounts must produce a greater balance of original content, and not simply reshare content from other accounts.

8. Closure of official Social Media accounts

8.1 The respective Corporate Communication department must be notified of the intention to close an account, at least seven days prior to deactivation / deletion / closure.

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

9. Personal Use of Social Media Sites

9.1 Social media users should note that some platforms, such as LinkedIn, encourage the disclosure of employers. It is recommended that personal and workplace content remains separate for your security.

9.2 Social media users should be aware that their use of social media in a personal capacity should always be compatible with this workplace policy.

9.3 Social media users should behave in a manner which does not discredit the police service or undermine public confidence in it, whether on or off duty - refer to Section 12 Breaches.

9.4 Any communications that individuals make in a personal capacity must not:

Bring either Force, or UK policing, into disrepute – this includes, but is not limited to;

• making defamatory or libellous comments about individuals, organisations or groups;

• posting images that are inappropriate or links to inappropriate content.

Breach confidentiality – this includes, but is not limited to;

• revealing confidential information owned by the Forces;

• revealing confidential information about an individual or organisation (such as a partner agency or other police force);

• revealing sensitive capabilities – both tactics and officer identities.

Breach copyright – this includes, but is not limited to;

• using third party images or written content without written consent; this includes the use of images or sound tracks that are not provided as part of the application, e.g. Tik Tok, downloaded from the intranet and internet;

• using trademarks or brands without permission. This includes the use of the crests or associated branding;

• failing to credit content where permission has been granted to reproduce it.

Breach the Data Protection Act 2018;

Be considered in any way discriminatory against, bullying of, or harassing of any individual – this includes, but is not limited to;

• making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion and belief, pregnancy and maternity, marriage and civil partnerships or age;

• using social media to bully another individual;

• posting images that are discriminatory or offensive (or links to such content).

Undermine the operational, investigative or criminal justice process – this includes, but is not limited to;

• being in contempt of Court;

• sharing intelligence or operational activities.

Be politically motivated, or make comment on any government policy that affects policing activity – local, national, or international – as UK police forces are apolitical organisations;

Involve contact with victims, suspects, or witnesses, met through work – this includes, but is not limited to;

• accepting friend requests, making friend requests, or commenting on public posts made by victims, suspects, or witnesses;

• any friend or contact requests received must be reported to Professional Standards Department (PSD) / Anti-Corruption Unit (ACU) to be considered as a notifiable associate.

9.5 Individuals should note that content used on social media can connect you to the policing sector, potentially increasing the risk to you, family and friends. The following are non-exclusive examples of content that can indirectly connect you to policing:

• the use of the 'thin blue line' symbol

• membership of policing specific groups or followership of policing specific accounts, for example Bullshire Police, UK Cop Humour etc.

• being tagged by friends and family members in statuses regarding policing or Force activity

• responding to posts or updates on official accounts from personal accounts that are not official individual accounts.

9.6 All staff are reminded that personal accounts or devices must not be used to provide updates, show evidence, or transfer files to members of the public or other partner organisations within the criminal justice system.

9.7 Organisational auditing software is in place in both Forces and should be used where a licence has been granted to a user.

10. Monitoring Use of Social Media

10.1 Official Force social media accounts can be accessed and reviewed by a user's supervisor. This can be undertaken through direct access to the account or through the Force's social media management platform.

10.2 Social media users should be aware that any official content, and content brought to organisational attention, may be monitored and, where breaches of this policy are found, action may be taken under Section 12.

10.3 Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us. It may also cause reputational damage to ourselves or UK Policing.

10.4 In particular, the uploading, posting, or forwarding of a link to any of the following types of material on a social media website, whether in a professional or personal capacity, may amount to Gross Misconduct (this list is not exhaustive):

• pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

• a false and defamatory statement about any person or organisation;

• material which is offensive, obscene, criminal, discriminatory, derogatory or may cause embarrassment to us, our staff, or victims of crime;

• confidential information about us, any of our staff, or victims of crime, which you do not have express authority to disseminate;

• any other statement which is likely to create any liability, whether criminal or civil, and whether for you or us; or

• any material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

10.5 Any such action will be addressed under section 12 Breaches.

10.6 If you notice any use of social media by other members of staff in breach of this policy it must be reported to your line manager, PSD directly, or via the Anonymous system in Surrey, and Break the Silence in Sussex.

11. Facebook Groups

11.1 Official social media accounts should not, in general, become members of Facebook Groups due to the risk posed to the Forces around unseen calls for assistance. The following exemption applies:

Where there is an operational requirement to enter a group to proactively tackle a reputational risk – for example an unauthorised encampment creating hyper-local community tensions. In these circumstances an exit strategy should be in place to exit the group at the soonest possible moment following the completion of the operational activity.

11.2 Local Policing Commanders (Chief Inspectors and Inspectors) should seek to build relationships with the administrators of influential, local community groups in order to provide support.

12. Breaches

12.1 Any breach of this policy should be reported to your line manager, Corporate Communications in the appropriate Force, PSD directly, or via the Anonymous system in Surrey, and Break the Silence in Sussex.

12.2 Breaches of this policy may be considered for investigation by the respective Force PSD.

12.3 Serious breaches of this policy, for example behaviour causing damage to public confidence in either Force; criticism of partner agencies, commercial organisations, or not-for-profits; cases of bullying colleagues; or other inappropriate comment in breach of the Code of Ethics may be considered Gross Misconduct. In particular such breaches may amount to Discreditable Conduct:

Police Officers (and Police Staff) behave in a manner which does not discredit the police service or undermine public confidence in it, whether on or off duty.

12.4 Questions regarding the content or application of this policy should be directed to the respective Force lead.

Team: Corporate Communications Department