Warwickshire POLICE	POLICY

Security Classification	**OFFICIAL**	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	**Mobile devices and social media policy**
REFERENCE NUMBER	**WP034**
Version	**3**

POLICY OWNERSHIP	
DIRECTORATE	ENABLING SERVICES
BUSINESS AREA	CORPORATE COMMUNICATIONS

INITIAL IMPLEMENTATION DATE	**16/03/23**
NEXT REVIEW DATE:	**16/03/26**
RISK RATING	**LOW**
EQUALITY ANALYSIS	**LOW**

Warwickshire Police welcomes comments and suggestions from the public and staff about the contents and implementation of this policy.
Please email policiesandprocedures@warwickshire.uk

Contents

1.0 POLICY OUTLINE

1.1 Mobile device usage and social media/online communications are key components to support the aims and objectives of the Fit for the Future strategy. Devices and social media/online communications undertaken on them support policing activity, operations and workforce collaboration. They enable us to communicate with the public, to be more active in our engagement and to improve confidence in policing.

1.2 Warwickshire Police provides officers, staff and volunteers with mobile devices such as laptops, tablets and mobile phones for policing work. These devices are the property of Warwickshire Police. It is the force's right to mandate how the devices are used, and the tools and platforms permitted on the devices.

1.3 Social media is the collective term for online tools, channels and interactive media that enable users to interact with others. Social media involves building online communities and/or networks which encourage participation and dialogue. Similarly, online communications use platforms for collaboration and sharing information via messaging or video. There is an extensive and ever-changing variety of tools and platforms available and covered by the scope of this policy. These include but are not limited to: Facebook, Twitter, Instagram, YouTube, TikTok, WhatsApp, Yammer, blogging sites and Microsoft Office 365 applications. For the purposes of this policy, the term 'social media' is used to describe all of these activities.

1.4 It is the force's right to mandate the type and nature of social media activities personnel may undertake for policing purposes and, where appropriate as set out below, for personal purposes that may affect Warwickshire Police in any way.

1.5 It is the responsibility of police personnel to use mobile devices in accordance with this policy, and to be accountable for their social media activity whether for policing or personal purposes.

1.6 This policy and the Code of Ethics and Standards of Professional Behaviour apply to police personnel in all social media activities, regardless of whether these are on Warwickshire Police-owned devices or not, and regardless of whether these are for police purposes or not.

2.0 PURPOSE OF POLICY

2.1 This policy brings together existing policies on social media and use of mobile devices. It also sets out the relationship between this policy and the force Lawful Business Monitoring policy, and it aligns with force Acceptable Use.

2.2 It aims to provide clarity (a) on the permitted use of mobile devices and (b), on the permitted type/nature of social media activities by personnel for policing purposes. This is with the intention of managing and minimising risk and enabling Warwickshire Police to use social media effectively, safely, appropriately, purposefully and legally.

It also aims to ensure that the use of social media by the force is in line with the national policing position, and with the Fit for the Future strategy.

2.3 It aims to ensure officers and staff are aware of their responsibilities regarding the use of mobile devices and social media, and are aware of the processes in place for the monitoring of mobile devices to identify and manage any misuse.

2.4 There is accompanying guidance online and provided through regularly scheduled training sessions to give an overview of social media channels and practices. This can be found via the Corporate Communications team intranet pages.

2.5 The Corporate Communications team and Digital Services provide guidance and support for the safe, appropriate and most effective use, respectively, of social media and mobile devices. The Professional Standards Department (PSD) manages adherence to policy and to the Code of Ethics and Standards of Professional Behaviour in line with The Police (Conduct) Regulations 2020 and The Police (Complaints and Misconduct) Regulations 2020.

3.0 IMPLICATIONS OF THE POLICY

3.1 It is anticipated that all personnel will adhere to the following procedures and policies alongside this policy:

a. College of Policing Authorised Professional Practice (APP): Engagement and Communication
b. Force Lawful Business Monitoring policy
c. Force IT systems policy
d. Force Acceptable Use policy
e. College of Policing Code of Ethics and Standards of Professional Behaviour
f. NPCC Guidance

3.2 The Code of Ethics and Standards of Professional Behaviour apply to all mobile device usage and social media activity for policing and personal purposes.

3.3 The Force has a legal right through its Professional Standards Department (PSD) to access force devices under the Lawful Business Monitoring policy at any time in line with this policy for a number of purposes including quality assurance, misconduct and criminal investigations. This right is set out in full in Section 4(2) of the Regulation of Investigatory Powers Act 2000 which gives the Secretary of State power to grant exemptions to businesses, including public agencies, around the monitoring and recording of communications made within their communications systems. These powers are contained within Investigatory Powers (Interception by Businesses etc for Monitoring and Record-keeping purposes) Regulations 2018.

3.4 Legal considerations also taken into account are The Human Rights Act 1998, The Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016, Investigatory Powers Regulations 2018, the General Data Protection Regulation (GDPR) and the Computer Misuse Act 1990. There are other risks attached to information sharing, however these should be proportionately and appropriately managed using the same principles that underpin all police activity.

4.0 MOBILE DEVICE USAGE

4.1 Each officer, member of staff or volunteer may have mobile device(s) allocated to them. The use of each device is restricted to the individual to whom it is allocated, and whoever uses a force-owned device must do so using their own login credentials. The allocated user is solely responsible for the use of mobile devices in accordance with this policy.

4.2 Telephone and messaging functions are available to use on smartphone devices, but personnel should not use these functions for premium rate numbers, overseas calls, use overseas or multimedia text messages. Personnel must secure line management, Digital Services and Force Vetting Unit approval for use overseas.

4.3 Devices with camera/video functionality can be used for evidential policing purposes but personnel are required to adhere to the following policies when using these:

a. Taking images with a corporate smartphone

b. Crime threshold for volume crime

c. NPIA professional practice advice on police use of digital images

4.4 The use of a device whilst engaging with the public, for example for note-taking/admin tasks during formal interviews is acceptable, but personnel should alert people present to the intention to use the device, should ensure other individuals cannot view sensitive information on the device, and should always consider the appropriateness of using a device to ensure it does not compromise the force's intentions to instil trust and confidence.

4.5 To connect to internet services safely and to prevent excessive use of phone data, personnel should always choose Wi-Fi over 3G/4G/5G, and should not usually connect via a "sign-up website" where name/email address/personal information/payment details are required. The only devices that can "tether' are force-issued laptops and force-issued mobile phones.

4.6 In accordance with force Acceptable Use, mobile devices should not be used for streaming video content unless for a specific policing purpose.

4.7 Personnel should ensure devices are well-maintained (including charging and storage), should take reasonable steps to reduce risks of theft or damage, should use passwords and the clear desk/clear screen requirements according to force Acceptable Use and should not alter the operating system or physical integrity of the device in any way. They should use approved cases supplied where applicable.

4.8 Personnel may download apps onto their device(s) via Google Play or via the force company portal. Only apps that are approved are available for download, and approval is subject to the role and responsibilities you hold. Personnel should contact Digital Services if they wish to request access to any unlisted app. This includes WhatsApp or other direct messaging services (see 6.5 for more detail on this).

The procedure for requesting a new messaging service on a work device is as follows:

a. Submit a request setting out the business need for access to the specific app to your Head of Department
b. Head of Department to consider application and submit to Digital Services if approved.

4.9 Personnel will primarily use mobile devices for everyday policing activities during working hours such as workforce collaboration, virtual meetings, corporate emails, file building, statement taking, visually recording evidence, engaging with victims and partners, managing police social media accounts and assessing corporate systems. Personnel should not use mobile devices for the sharing of offensive/lewd images, messages or videos via any platform or account and they should not use mobile devices for dating, gambling, shopping or auction sites.

4.10 Personnel may make reasonable use of their mobile device(s) for personal purposes during duty hours and time away from work. Purposes may include checking/sending personal messages and calls, monitoring the news, checking the weather, checking fitness and promotion studies. Reasonable use is judged on a case-by-case basis with the following considerations:

a. the full circumstances of the situation
b. the frequency of use
c. the Code of Ethics and Standards of Professional Behaviour
d. how usage may appear to the public (see 4.4)

4.11 Mobile devices are intended to support effectiveness and efficiency, and can improve work-life balance where used appropriately. Managers should be aware of agile working procedures and optimise the benefits of the force's policy for all personnel, without any continued or unreasonable expectation that personnel will need to use mobile devices out of working hours.

4.12 Personnel are not permitted to divert their work mobile phones to personal mobile phones due to the risks of policing information being accessible to hostile third parties, network compromise, contravention of business insurance and contravention of ICO requirements via personal devices - putting the individual or force at risk (see section 5 and the Warwickshire Police Lawful Business Monitoring Policy and Procedure and force Acceptable use).

5.0 WORK ISSUED MOBILE DEVICES DOWNLOADS

5.1 This policy should be read in conjunction with the Lawful Business Monitoring Policy, which allows for the monitoring and recording the use of force communication systems - incorporating calls, text messages and other communication methods.

5.2 Lawful business monitoring allows Warwickshire Police to monitor, retrieve, intercept and store any activity undertaken on force-issued devices or via force-issued services. Devices include laptops, mobile phones and radios, and services include, but are not limited to, email, social media apps, telephone systems and Office 365 programmes. Activity includes for any policing purposes and for personal purposes when these are carried out on force-issued devices (see 4.10).

5.3 Personal information may be viewed in alignment with lawful business monitoring processes if this is on a force-issued device.

5.4 For mobile device downloads, the procedure will entail business areas and personnel chosen at random. They will be consulted on availability, and will be mandated to provide the Professional Standards Department with their mobile device(s) with full access and password protection removed. The device(s) will be downloaded by a qualified Anti-Corruption Unit Digital Media Investigator (DMI) or other DMI as appropriate, and returned when the download has been completed and examined.

5.5 Failure to provide the device, and any breaches of the Standards of Professional Behaviour and/or Code of Ethics identified from the download, will be assessed in line with conduct regulations.

6.0 SOCIAL MEDIA FOR POLICING PURPOSES

6.1 The force's activities on social media should engage our workforce and communities through information, dialogue and inspiration with the strategic aim of building trust and confidence. It is critical that anyone undertaking social media activity as part of Warwickshire Police supports this endeavour with every item they post.

6.2 Personnel should apply the same professional standards and ethics to their social media communications and activities in online forums as they would to face to face, telephone or any other interactions. The Code of Ethics and Standards of Professional Behaviour applies to police personnel in their use of social media whether this is for policing purposes or personal use.

6.3 Content, comments or posts on social media must not:

a. Undermine operational, investigative or criminal justice processes;
b. Contain information, imagery or video which is protectively marked, could breach confidentiality or data protection laws;
c. Breach copyright laws;
d. Divulge sensitive operational and covert tactics;
e. Provide details of an investigation or operation without SIO approval;
f. Make defamatory, libellous, discriminatory or bullying comments;
g. Be capable of bringing Warwickshire Police and policing into disrepute, damage reputation or undermine public confidence.

6.4 The Corporate Communications team defines the social media channels to be used by the force depending on campaign, audience, purpose and type of content.

Information on channels and support available to use social media is outlined in the accompanying guidance.

6.5 Police information should only be sent via Force-approved social media channels, platforms and services. These are defined on the Corporate Communications team intranet pages and the apps available to personnel to download on force-issued devices. WhatsApp, Facebook Messenger, Twitter DM, Snapchat and any other direct messaging services are not approved for the communication of police information on work-issued devices or personal devices. See 4.8 for information on requesting access to other services. Such information should also only be shared with those who require it and have the authority to view it. Collaboration for policing purposes should be kept separate from any social groups on any platform. All personnel are responsible for the information they disclose in accordance with the Data Protection Act 2018.

6.6 All departmental social media accounts must be approved and set up by Corporate Communications. Corporate Communications may access any force social media account for monitoring, management or engagement in line with this policy, and must have an up-to-date record of log-in details in order to access accounts.

6.7 Responsibility for the day-to-day management of departmental accounts rests with individual teams under the supervision of the team manager. Teams must maintain an accurate record of personnel authorised to use the account, which should be shared with Corporate Communications. All accounts should contain signposting to appropriate channels for emergencies and reporting crimes, and teams must respond to questions, comments and concerns where appropriate.

6.8 Responsibility for the force's corporate communications response to major incidents sits with Corporate Communications, who will use all corporate channels to ensure consistency in public information and messaging, and will provide guidance to departmental account holders on content to publish, monitor or pause where appropriate. During such an incident, other content may be paused to ensure messaging is not diluted. Via the Corporate Communications out of hours rota, the team is also responsible for 24/7 advice and guidance in relation to any urgent or critical issues with social media.

7.0 PERSONAL SOCIAL MEDIA USE

7.1 It is recognised and accepted that police officers, staff and volunteers will use social media channels in their personal lives. Hostile third parties take a keen interest in the information contained in social media profiles – in any format, whether it be words or pictures, that provides an indication of an individual's position in the police and the level of access to information that individual may have, and this may put an individual, and the force, at risk of potential harm. There is also risk of breaching the Code of Ethics. Personnel are therefore expected to take reasonable steps to protect themselves and the reputation of Warwickshire Police online. This includes using appropriate security settings on social media platforms**.**

7.2 Individuals must not share information related to policing operations via their personal social media accounts, and are advised not to share personal details, address details and specific details of their association with the Police. Any images of individuals in Police uniform on personal accounts should comply with the Code of Ethics and should not be damaging to the reputation of the force. Individuals must never reveal their security clearance (vetting) level or that of any other personnel, and they must ensure that they make clear in any social media activity including profiles and postings that they are speaking on their own behalf, not on behalf of Warwickshire Police.

7.3 Individuals should be mindful that the content of online private or group chats may not remain private. Individuals are responsible for moderating their online communications and group membership and should leave groups where communications are not acceptable within the scope of this policy and the Code of Ethics and Standards of Professional Behaviour. They should report such activity in line with Warwickshire Police's 'Professional Standards Reporting Procedure' (see Procedure for further details).

7.3 Online associations must be considered in the same way as in person and individuals should be mindful of their associations on social media platforms, including on LinkedIn, to ensure there is no compromise to policing operations or their position at Warwickshire Police. If an online association through social media falls within a category listed in the Notifiable Associations Policy, personnel should declare these as appropriate accordingly.

7.4 Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with duties and responsibilities or productivity and adheres to this policy.

8.0 INAPPROPRIATE USE OF SOCIAL MEDIA

8.1 Inappropriate use of social media accounts by personnel, via force or privately held accounts, may warrant formal action being instigated by Professional Standards in accordance with criminal or misconduct proceedings.

8.2 If inappropriate, offensive or illegal comments or complaints are posted on Warwickshire Police social media channels by members of the public, these should be considered by the individual's supervisor or line manager in the first instance to ensure wellbeing support for the individual and investigation as appropriate. The channel administrator/account holder should alert Corporate Communications who will advise on appropriate measures. If the comments are considered to fall under the Home Office Counting Rules definition of Hate Crime or malicious communication, they will be referred to the Resolution Centre.

9.0 LOG-IN CREDENTIALS AND PASSWORDS

9.1 Due to the risks of compromise to policing information and reputation through hostile access to log-in credentials, passwords and mobile devices, personnel should take reasonable care with the information they use to access all online platforms, including social media. This means that they should not use common passwords across multiple systems/sites/devices and should not use credentials used for police systems or mobile devices for other platforms/devices.

10.0 CONSULTATION

10.1 The approach to adopt the original social media policy was agreed by the Executive Board in May 2013. It was reviewed by Corporate Communications professionals and the Head of Corporate Communications in September 2016, again in September 2018 and again in October 2020.

10.2 The mobile devices, social media and lawful business monitoring policies were originally designed following consultation with subject expert teams and Chief Officers. This integrated policy has been created following consultation with Corporate Communications, Digital Services and the Professional Standards Department. It continues to follow national guidance from the College of Policing's APP and the NPCC.

11.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

Date	Author / Reviewer	Amendment(s) & Rationale	Approval / Adoption
July 2013	Head Cop Comms 4643	Harmonisation	JNCC 13/09/2013
Sept 2016	Head Cop Comms 4643	Review – Content unchanged appendix 1 minor adjustment v1.1	16/09/2016
August 2018	Dept Head Corp Comms. 5739	Review -Document updated to reflect NPCC social media approach, developments within the Corporate Communications function and to cover personal use of social media by alliance personnel v1.2	JNCC 11/12/2018

Nov 2020	Dept Head Corp Comms. 5739	Review – document updated to reflect alliance separation, new guidance in place for use of WhatsApp and to align with future changes to relevant legislation.	25/11/2020 Minor Changes approved
Sept 2021	Internal Comms & Engagement Officer 6718 Dept Head Corp Comms. 5739	WhatsApp guidance updated	29/09/2021 Minor changes
May 2022	Dept Head Corp Comms. 8191	Review – document updated to reflect introduction of MS Teams for online communications, to align with updates to relevant legislation and best practice from NPCC, to integrate with mobile devices policy and lawful business monitoring and to align with acceptable use policy.	
October 2022	Dept Head Corp Comms. 8191	Amendments made following review by Executive Board.	22/03/23