



Force Issued Electronic Devices Policy (Surrey and Sussex) (1177/2024)

Abstract

This policy details how Force issued electronic devices must be utilised for accessing information and approved applications, and how such information should be managed securely.

Policy

1. Introduction

1.1 The purpose of this policy is to ensure Surrey Police and Sussex Police (hereafter referred to as the Forces) issued devices are used correctly to maximise operational use, and that all individuals coming into contact with a device, or material contained on the device, are able to comply with legislation and the Force's requirements. In addition, individuals issued with a Force's electronic device as part of their work and operational duties must be aware of their responsibilities in relation to its use and care.

1.2 Unless specifically noted, any reference to 'users' within this document applies equally to police officers and police staff.

2. Scope

2.1 This policy covers all aspects of the usage, storage, management, and security of a Force issued electronic device, and how to deal with faults, damage, or the return of equipment.

3. Policy Statement

3.1 The Forces expect all users to safeguard Force property and to ensure the integrity of Force applications and information are not compromised.

3.2 The Forces are committed to making best use of their resources by taking full advantage of new technology in all appropriate circumstances.

Procedure

1. Introduction Overview

1.1 The following is applicable regardless of whether or not the individual is on duty.

1.2 These procedures have been designed with regard to current legislation and guidance.

1.3 All police officers and police staff receiving a Force issued device will have a sound business case for allocation. As such, high level usage for policing purposes is expected,

both when in private and also when in public view. Force communications via relevant media channels will ensure users have support to be seen visibly using a device in public.

2. Definitions

2.1 Force Issued Electronic Device:

- Any electronic device (including smartphones, Mobile Data Terminals (MDTs), tablets, laptops), issued by the Forces for voice calls, SMS, Video, and connection to Force (or National) information systems. This does not include Body Worn Video (BWV) which is subject to a separate policy.

Accessories that may be issued, for example;

- Charger (Standard 240V to 5V 2amp Charger)
- USB cable
- Protective case
- S-Pen (small plastic pen that comes with some smartphones) / Stylus
- Portable Bluetooth keyboard

3. Devices

3.1 The device, its content and all its accessories are owned by the Forces.

3.2 The SIM card provided must not to be used in any other device other than that issued by the Forces.

3.3 No SIM card other than that issued by the Forces will be used.

3.4 Police officers and police staff must abide by legislation regarding the use of mobile phones while driving.

4. Security

4.1 Frontline officers are reminded to remain situationally aware at all times, particularly when using mobile devices in a public place.

4.2 Users must not leave their device unattended in a public or insecure location.

4.3 Users must ensure that when they are using their device in a public place, they are positioned as such to prevent unauthorised persons viewing the screen, and that their personal information and passwords are not visible to members of the public when being entered into the device.

4.4 Users must exercise caution in respect of any vulnerability of unauthorised access to the device via Bluetooth. This function is to be disabled unless being utilised for a policing purpose e.g., with a portable keyboard, connection to hands free systems.

4.5 Users must understand that any telephone conversation using a Force device cannot be considered to be 'secure' as it may be possible for others to overhear conversations that could result in the unintentional passing on of sensitive information.

4.6 Each device is personal issue for use with an individual's Force network domain account. All work shall be carried out using this account, and the device must not be shared with any other individual.

4.7 The Forces reserve the right to perform a full remote wipe of a device if necessary to ensure the protection of Force data.

4.8 The device uses encryption to ensure any approved apps are secure. Users must not use any other apps to record notes or other investigative details. Users are reminded that under the [Criminal Procedure and Investigations Act 1996](#) all information gathered as part of an investigation must be recorded, retained and revealed as part of the disclosure process; this will include information on a Force issued device.

5. Maintenance and Care

5.1 It is the responsibility of the user to look after the device and accessories supplied. Loss of a device could lead to a breach of security and must be reported immediately via the Security and Breach Reporting Portal and your line manager.

5.2 Any breaches of personal / sensitive data must be reported to the relevant Force Data Protection Officer within 72 hours as the Information Commissioners Office (ICO) has powers to impose greater penalties. These breaches must be reported using the Security and Breach Reporting Portal and your line manager.

5.3 Users must take all reasonable measures to ensure the device and accessories provided are not lost or damaged. Where a device is lost users must report the loss via the Security and Breach Reporting Portal or where a device is damaged, users must contact the IT Service Desk.

5.4 If the loss or damage is deemed to be deliberate or reckless, then the Professional Standards Department (PSD) will be notified.

5.5 Any faults must be reported to the IT Service Desk.

5.6 Devices are assigned to specific individuals for work purposes only and should not be loaned to, or used, by any other individual.

6. Use

6.1 Users are only permitted to use their Force issued device for personal use in an emergency when no other communication option is available. The device is a Force asset, when the device is used for a personal purpose all users must understand personal use is subject to the restrictions and controls outlined in the relevant acceptable use guidance and information management policies and should refer to Section 10 within this Policy. Regular use of a Force device for personal communication is not permitted.

6.2 Voice calling and data activity must be restricted to UK networks and does not include "premium rate" or otherwise "chargeable" numbers. Excessive or chargeable use will be investigated.

6.3 Taking a Force electronic device outside of the UK is not permitted without authorisation from PSD. Where authorised, IT Department must be notified.

6.4 Use of a Force issued electronic device, and any data captured by or held within the device remains the property of the Forces, and therefore subject to professional standards. This includes photographs, videos, emails, and data held within applications.

7. Policing Applications

7.1 It is the responsibility of the individual user to ensure they are fully aware of and comply with the related guidance and policies associated with access to Force's systems.

8. WhatsApp

8.1 Use of WhatsApp has now been approved for use for work purposes and can be used, at the user's discretion, to contact work colleagues and members of the public and is a tool that is available for one or both of these purposes. Users should be advised that WhatsApp may not always be made available and is under constant review. Users should therefore not depend on the service to carry out business and be prepared for any adjustments that may be necessary in the event WhatsApp is withdrawn from Force usage.

8.2 This application will be available to download directly through the Corporate Application Store on your device.

8.3 In order to ensure that both users and communications are secured and safeguarded appropriately all users must ensure that the FSecure App on the MDT devices is installed and switched on prior to use of WhatsApp. Any conversations must not be 'mirrored' to an alternative 'linked' personal device. For example, conversations on a Force issued mobile phone must not be mirrored to a personal phone. This will prevent unauthorised disclosure of police information.

8.4 The following settings must be enabled in WhatsApp prior to its use and failure to do so will be in breach of this policy;

redacted

- The following two phone numbers must be added to the phone's "contacts" in order to receive corporate message broadcasts about the use of WhatsApp:

- Surrey Corporate Communications: redacted

- Sussex Corporate Communications: redacted

8.5 Due to the nature of how this platform operates, under no circumstances will sensitive information be shared. Sharing operational or sensitive information through WhatsApp is a clear breach of our information management policy and appropriate action will be taken.

8.6 The only exception is for time critical essential operational reasons for which no appropriate alternative communication means can be found and where the information shared must be kept to a minimum and internal to the police only. This material must be deleted as soon as the policing purpose has concluded, with participants limited to need-to-know individuals.

8.7 Should you receive a message that is not from a known source please delete the message rather than opening it, especially if the message has an attachment (a video or image for example).

8.8 WhatsApp Groups

- Ensure that a designated, documented individual is responsible for group management adding legitimate and authorised users and revoking access when it is no longer necessary.
- Should you consider that there is no longer a specific policing purpose in remaining within any given WhatsApp group, you must leave it immediately
- Should you suspect any behaviour in a group is an inappropriate use of the group or a breach of the standards of professional behaviour, this must be reported and challenged. Staff and officers have a duty under the Standards of Professional Behaviour to report and challenge inappropriate comments and behaviour. All discussion on Force devices is subject to the same scrutiny as any other platform where users represent Surrey Police and Sussex Police. Maintaining professionalism in all conversations is a requirement. And you must keep the content for later viewing by PSD.
- You must avoid creating “groups” that are a combination of police officers, police staff and members of the public, to minimise the risk of public coming into contact with “police language” or sensitive information.
- Users must personally consider whether it is appropriate to join any WhatsApp group that they are invited to join (whether created by a member of staff, or a member of the public) and should ensure you are clear about the purpose of the group, and who is a member of that group before posting.
- Users must be aware of the risk of any member in a group being able to identify any other member’s phone number by virtue of the fact that they are in the same group. For this reason you must consider very carefully the need for setting up a WhatsApp group that includes members of the public.
- You may choose to signal which groups are “police only” by prefixing the group name “police” or use a police car Emoji sign.
- Although WhatsApp allows multiple administrators for WhatsApp groups, it is mandated to only have designated, documented individuals responsible for admin for each group used for policing purposes. Those persons being solely responsible for managing the group.
- Users must take particular care that conversations with victims and conversations with suspects are kept completely separate at all times.
- Any conversation could be subject to release under Disclosure or Freedom of Information (FOI). Conversations can be quickly exported under “settings” for each group or conversation.
- Cloud repositories such as iCloud must not be used to store conversation histories with colleagues or members of the public as these environments are not assured and could

be subject to a data breach. If this information is needed for a policing purpose content must be sent to a user's Force email account.

- Regular refreshment of conversation histories should be undertaken at least annually to remove all content where the policing purpose has expired
- Ensure that the latest version of WhatsApp is downloaded onto a user device, as this will act as a safeguard against potential hacking
- No user profiles are to be 'merged' with any other social media platform such as Facebook or Instagram. No material will be shared via any additional functionality added to the application.

8.9 WhatsApp Contact Lists

All device users must update their contacts to remove personal contacts within Force Mobile Devices that are not required for an operational need. This can be done in one of the following ways:

1. Download the new MINT extract data from SnapShot Mint for Samsung (SUSSEX only). IT have implemented a solution which has removed personal contact details from the MINT extract. Please follow these instructions to complete this found on the intranet.
2. Complete a manual check of your contact list and manually delete personal contact details

There may be an operational need to have contact with a member of the public / external contacts and store their number to a Force Mobile Device. If this is the case, contact must be initiated as follows in order to comply with UK General Data Protection Regulations (GDPR) and Data Protection Act (DPA) 2018:

- Surrey / Sussex Force Mobile Device user provides their Force Mobile Device number to the member of the public / external contact
- The member of the public / external contact generates a WhatsApp chat with the Surrey / Sussex Force Mobile Device user on the number that was provided to them. By the contact being generated in this way they have provided their own details to WhatsApp which complies with UK GDPR and DPA 2018.
- The Surrey / Sussex Force Mobile Device user can then save the contact details of the member of the public / external contact to their device to identify them within this chat.

Device users must periodically check their contacts and remove personal contacts within Force Mobile Devices that are no longer required for an operational need.

8.10 WhatsApp is a commercially offered service which is not designed for use within a corporate setting and is subject to changes and developments outside of the control of the Forces.

8.11 Access to WhatsApp remains under review and the Forces will not hesitate to remove access either individually or organisationally if circumstances deem it appropriate. These circumstances may include:

- Misuse of the service by an individual

- A change to the service offered that changes the risks associated with the service or materially changes the function of the service
- National guidance changing or
- A similar service which is designed for use within a corporate setting becoming available.

8.12 Access to WhatsApp web version and WhatsApp desktop version must only be made through Force issued computers.

9. Third Party Applications 'Apps'

9.1 Third party applications will be made available to users for download via the application catalogue on the device. Only approved applications can be downloaded.

9.2 When using any third party applications, the same acceptable use guidance applies as per the policing software applications.

9.3 Social media web and mobile apps such as Facebook, WhatsApp and Twitter are made available for use with Force approved accounts. Users must not use their own personal accounts.

9.4 Users must not upload or share any restricted information or material using a third party application (e.g. any social media applications, or third party media storage applications).

9.5 It is the responsibility of the individual user to ensure they are fully aware of and comply with the related guidance and policies.

9.6 Any access to the internet using a Force issued device must comply with any current Force Internet Security Guidelines.

9.7 Device cameras can be used in an operational context in any approved App. However, any photos required for evidence gathering must be captured in the Pronto app in order for them to be used for evidential purposes. Video footage must not be taken due to difficulties in recovering this from devices and BWV must be used for this. Any images captured must be treated according to Force policy.

9.8 Users of corporate smartphones will be expected to comply with the requirements of other organisations regarding use of these devices within their premises (e.g., medical facilities).

9.9 Some applications give the ability to record members of the public and telephone conversations. Under Regulation of Investigatory Powers Act 2000 (RIPA) section 3(1) this is lawful where both the sender and intended recipient of the communication give their consent to the interception the beginning of any conversation it is made clear the conversation is being recorded so there can be no misunderstanding.

10. Privacy

10.1 Users of Force issued electronic devices should have no expectations of privacy in respect of the use of their device. All activity, including, but not limited to, call costs, numbers dialed, and data usage (including browser activity) will be liable to monitoring for

management purposes and in order to ensure compliance with the Code of Ethics and Force policies.

11. Related Documents and Legislation

11.1 Surrey Police and Sussex Police Information Security Policy (722)

Lawful Business Monitoring Policy (Surrey and Sussex) (1196)

Information Management Policy (Surrey and Sussex) (1187)

Data Protection Policy (Surrey and Sussex) (780)

Data Protection Breach Policy (Surrey and Sussex) (1180)

[Data Protection Act 2018](#)

[Criminal Procedure and Investigations Act 1996](#)

[Computer Misuse Act 1990](#)

Team: Digital Data and Technology