

MOBILE DEVICE USE POLICY

Official



MOBILE DEVICE USE

Owning Department: Joint ICT

Department SPOC: Chief Digital Officer

Risk Rating: Medium High

Legal Sign Off: 15.11.2023

JNCC: 30/08/2023

Published Date: 15/11/2023 (V3)

Review Date: 03/09/2026

Official

Version Number: 3

Page 1 of 12

MOBILE DEVICE USE POLICY

Official

Index

1. Introduction	3
2. Statement of Policy	3
3. Applicability	4
4. Device Deployment	4
5. User Responsibilities	4
6. Incident Response	5
7. Mobile Working Expectations	5
8. Passwords	6
9. Voicemail	6
10. Wi-Fi	7
11. Tethering	7
12. Bluetooth	7
13. Social Media	8
14. Email	8
15. Internet Use	8
16. Applications / Services	8
17. OPTIK	9
18. Digital Images	9
19. Prohibited Activities	9
20. Monitoring	10
21. Personal Data	11
22. Device Management, Transfer and Return	12

Legal Basis

Legislation specific to the subject of this policy document:

- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000

Other relevant legislation which you must check this document against (required by law)

- Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
- Equality Act 2010
- Crime and Disorder Act 1998
- Health and Safety at Work etc. Act 1974 and associated Regulations
- General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Freedom Of Information Act 2000
- The Civil Contingencies Act 2004

Other documentation which you must check this document against:

- College of Policing – Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- College of Policing – Authorised Professional Practice

Official

Version Number: 3

Page 2 of 12

MOBILE DEVICE USE POLICY

Official

Other related documents

- Information and Cyber Security Incident and Data Breach Reporting and Management Policy and Procedure
- Digital Engagement and Social Media Policy
- Provision of ICT Equipment
- Acceptable Use of Information Systems and Assets Policy
- Acceptable Use of Information Systems and Assets Procedure
- Acceptable Use of Instant Messaging Procedure
- Maternity Leave (Officers)
- Maternity Leave (Staff)
- Disciplinary (Police Staff)
- Misconduct – Police Officers
- Adoption Leave Staff and Officers
- Career Break Staff and Officers
- Secondments
- Email, Internet and Intranet Use Policy
- Email, Internet and Intranet Use Procedure

1. Introduction

- 1.1 The purpose of the policy is to provide users of mobile devices (“users”) with clear guidance on their responsibilities and the protocols to follow when equipment is lost or damaged.
- 1.2 All police officers and police staff using mobile devices issued by Norfolk and Suffolk Constabularies (together “the Constabularies” and/or “Forces”) have a responsibility to adhere to this policy and the procedures within.
- 1.3 Personal issue will refer to a mobile device that has been issued for the exclusive use of an individual.
- 1.4 The aim of this Mobile Device Use Policy is to ensure that:
 - Devices are appropriately operated;
 - Correct procedures are followed in the event of an unexplained malfunction of the device, or other security incidents (such as suspected mobile device tampering or loss);
 - Users have a good understanding of the security functionality of the devices.

2. Statement of Policy

- 2.1 This policy has been formally agreed via the approved policy development/review process. It will be maintained by the ICT Department in conjunction with the Central Policy Unit.

Official

Version Number: 3

Page 3 of 12

MOBILE DEVICE USE POLICY

Official

- 2.2 The policy is intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status.
- 2.3 Managers have a responsibility to ensure this policy and its associated procedures are applied fairly, and unless otherwise stated, all policies and procedures are non-contractual

3. Applicability

- 3.1 Unless otherwise stated, this policy applies to all police officers (including officers of the Special Constabulary) and all members of police staff (including police support volunteers).

4. Device Deployment

- 4.1 The purposes of the deployment of mobile devices across the Constabularies are:
- To enable officers and staff to work more effectively with real time and easy access to Force systems, reducing the amount of time spent in police stations;
 - To enable easier access to colleagues and the public for officers and staff; and
 - To enable officers and staff to work in a smarter and more cost-effective way.

5. User Responsibilities

- 5.1 Users should follow these procedures at all times while operating the device issued to them by the Force (“their device”). Failure to comply with these procedures may result in disciplinary proceedings.
- 5.2 All users must read, fully understand and accept the procedures and advice in this document. Before using their device, users will be required to sign a Terms and Conditions document.
- 5.3 Users are responsible for the physical security of their device and must be aware that failure to follow these procedures could lead to compromise of not only data stored locally on the device, but also the police network they are connecting to.
- 5.4 When using their mobile device, users must ensure that it is not possible for bystanders to view classified information on the display, or to observe the device password being entered.
- 5.5 Mobile devices may be a target of theft. In addition to the obvious inconvenience of having a device stolen, there is also a risk of sensitive data being extracted. Users should therefore take all possible measures to avoid their device being stolen; it must never be left unattended in unlocked police vehicles, on desks in unsecure open offices, hotel rooms, or on view at home, etc.
- 5.6 Users must not allow anyone else to use their phone or tablet as there is a risk that they could modify device settings in order to render the device vulnerable to further attack.

Official

Version Number: 3

Page 4 of 12

MOBILE DEVICE USE POLICY

Official

- 5.7 It is the user's responsibility to ensure the device remains charged whilst on duty/within their working day and is fully charged at the start of each shift.
- 5.8 Users must not attempt to run unsigned code (e.g. jailbreak) and/or operating systems/applications not approved by ICT or otherwise circumvent security controls on the devices. Any such attempt will be regarded by Norfolk and Suffolk Constabularies' Professional Standards Department as a disciplinary matter and, potentially, a contravention of the Computer Misuse Act 1990.

6. Incident Response

- 6.1 If their device is believed to be lost or stolen, users must immediately notify the ICT department via the Service Desk (x4747). If out of hours, users should contact the Force Duty Officer (Oscar 1) located in CCR. Oscar 1 will then get in touch with the relevant on call team to respond and action.
- 6.2 Reports of this type of incident should be made immediately and prior to a protracted search.
- 6.3 In addition to a report being made to ICT, any device that has been lost MUST be reported to Information Security via an Information Security Incident Form, in line with the Information and Cyber Security Incident and Data Breach Reporting and Management Policy and Procedure.
- 6.4 If users believe that their password has been compromised, it must be changed immediately.
- 6.5 If a user forgets their device password, they should contact their ICT Service Desk and have their identity confirmed prior to a password reset taking place.
- 6.6 If the device stops functioning as normal, users must contact their ICT Service Desk. The device must not be given by the user to a third-party (e.g. commercial repairer) to rectify any issues. Users must not tamper or dismantle any issued device.
- 6.7 If a device shows signs of having been tampered with, the user must stop using it immediately, switch it off and inform the ICT Service Desk.
- 6.8 Hardware issues, for example cracked screens or broken cases, must be reported to the ICT Service Desk in the first instance.

7. Mobile Working Expectations

- 7.1 There is no expectation or work-related requirement for users to use any devices whilst off duty or outside of working hours.
- 7.2 The devices will allow users access to emails away from a work environment or at home; this is a personal choice and time away from work (rest days or annual leave) should be not be used to excessively check the devices.
- 7.3 Officers and police staff will not be classed as being on duty if they do check emails or carry out other administrative tasks, unless the need to do so is necessary as part of a live incident or urgent matter.

Official

MOBILE DEVICE USE POLICY

Official

- 7.4 In addition to the above, there is no expectation for officers or staff to have any devices accessible off duty unless as required for on-call duties.
- 7.5 Access to any Force systems or data whilst off duty **MUST** only be for a genuine policing purpose and should not be used to update friends/family or associates on an investigation or incident. Such enquiries should be directed to the OIC. For further information relating to information access, please refer to the Acceptable Use of Information Systems and Assets Policy (and Procedures).

8. Passwords

- 8.1 It is important that a strong password is chosen by users, i.e. one that is difficult to guess. In the event of the device being stolen or found by a member of the public, a weak password could make it easier for sensitive data on the device to be accessed.
- 8.2 Unless advised otherwise, users' passwords must meet the following requirements:
- It must contain a mixture of upper-case and lower-case letters, numbers and special characters and minimum of nine characters in length;
 - It should not contain recognisable words, or any other strings associated with the user.
- 8.3 Users must never disclose their device password to anyone (including those on the ICT Service Desk), either in person, by phone, or by email/text messaging.
- 8.4 This password requirement will be enforced by the Mobile Device Manager.
- 8.5 Users will be able to choose between unlocking the device via password or fingerprint. After restarting the device or after a period of inactivity, a password will always be required.
- 8.6 For security purposes, after 5 wrong attempts the device will be wiped. If users are down to the last remaining attempt and they are unsure of what their password is, or the fingerprint reader is not working, they should contact the ICT Service Desk.
- 8.7 Further information on the Constabularies' Password Policy can be found within the Acceptable Use of Information Systems and Assets Policy.

9. Voicemail

- 9.1 With the exception of officers working in covert units, all users must set up a personal voicemail answer message when they receive a device that can receive calls. Advice on how to do this will be available via the self-help area of the intranet.
- 9.2 Voicemail should not be used as a call filtering service; if members of staff or officers are available to answer calls, they should do so.
- 9.3 Accessing voicemail recordings other than an individual user's own is not permitted and would be considered a breach of this policy. Any request to access another

Official

MOBILE DEVICE USE POLICY

Official

member of staff's voicemail must be by request to the Joint Information Security team.

- 9.4 Voicemail greeting messages should be updated regularly, especially for periods of extended absence. Additionally, alternative contacts should be provided where possible.
- 9.5 Voicemail messages should be checked as soon as possible after returning from a period of leave.
- 9.6 Voicemail greeting messages should include the following:
- The user's name (including department and organisation);
 - When the caller can expect a return call;
 - Name and contact number of a colleague who can provide assistance if the user is unavailable;
 - That 999 should be used in case of emergency.

10. Wi-Fi

- 10.1 The devices will connect to Wi-Fi networks and hub equipped vehicles. The devices will not connect to public Wi-Fi hotspots such as those found in coffee shops and hotels.
- 10.2 Where the Constabularies' Corporate Wi-Fi connection is available this should be used in preference to any other Wi-Fi networks.
- 10.3 ICT security protocols will block any unsafe connections. Connection to private internet hubs is permitted when permission is given.

11. Tethering

- 11.1 Tethering should only be used when a secure Wi-Fi connection is unavailable.
- 11.2 Tethering should only be used to share an internet connection from a Force issued device (e.g. a smartphone or tablet) to a Force issued laptop and should not be used for the connection of a personal device.
- 11.3 Where the user changes the device's hotspot name from the automatic generic name; this should not attribute the hotspot to a Constabulary issued device and/or the user.
- 11.4 Where the user changes the automatically generated hotspot password, this should be changed to a strong password that is a minimum of 8 characters with a mixture of upper- and lower-case letters, numbers and a special character.

12. Bluetooth

- 12.1 The devices are enabled for the use of in-car Bluetooth but not for the transfer of data.

Official

MOBILE DEVICE USE POLICY

Official

13. Social Media

- 13.1 Access to official Norfolk and Suffolk Constabulary social media accounts, such as Twitter and Facebook, will be possible for users from the devices, if authorised. The existing Digital Engagement and Social Media Policy should be referenced for terms of use.
- 13.2 Personal social media accounts must not be accessed via a device issued for work use.

14. Email

- 14.1 The devices will enable the user to access their Force email account. Use of Force email is as per current Acceptable Use of Information Systems and Assets Policy. The content of emails is subject to audit and monitoring.
- 14.2 Users will not send any communication from the phones or tablets that are beyond the permitted level of the devices under the Government Security Classification which is currently 'OFFICIAL'. Correspondence received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements.
- 14.3 Users are able to send and receive emails that contain attached documents such as Word, Excel or image files. These attachments may be opened on the device, provided they come from a recognised source. Email attachments from unrecognised sources, a file type not known, or which are not expected should not be opened on the device and referred to ICT for further help and support.
- 14.4 When off duty or on annual leave, users should ensure that their 'Out of Office' for email is on and bears the agreed format of message.

15. Internet Use

- 15.1 The devices will allow access to the Internet and users will be subject to the same level of monitoring, moderating, supervision and web marshalling as with normal desktop use.
- 15.2 Users will be allowed to use the internet during work time for policing purposes; it must not be used for personal browsing and must not expose Norfolk or Suffolk Constabularies to reputational risk.

16. Applications / Services

- 16.1 The devices will come with a number of applications and services already installed. Further applications that have been authorised for use can be found in the 'Links' app installed on the phone or from the Playstore application on the device.
- 16.2 If an application which has not been authorised for use is identified as beneficial, then this should be requested via the ICT Service Desk for further assessment and consideration.
- 16.3 Users will be notified whether an application has been approved or declined once a decision has been made.

Official

Version Number: 3

Page 8 of 12

MOBILE DEVICE USE POLICY

Official

17. OPTIK

17.1 OPTIK will be the assumed default method of carrying out processes contained within the OPTIK mobile application. Only in the event of OPTIK downtime, device failure or operational needs should paper, or alternative methods be used. Business continuity plans for such event can be found on the Learning and Management System (“LMS”).

17.2 Only Force approved ancillary devices, such as the Crossmatch Nomad 30 Mobile ID scanners, are permitted to be connected to a Norfolk and Suffolk Constabulary mobile device. Mobile ID scanners should be used in accordance with the Standard Operating Procedure (“SOP”), which can be found on the LMS.

17.3 Officers and staff should ensure that they have:

- Conducted any Force approved training required to operate the core systems that OPTIK interfaces with; and
- Familiarised themselves with the OPTIK training videos that are located on the LMS.

18. Digital Images

18.1 Officers and staff must use the ‘National Decision-Making Model’ (NDMM) to decide when and in what circumstances to capture a Digital Image of a person. This will only ever be for a legitimate policing purpose.

18.2 It is not permissible to take a photograph of someone where their ID has been positively corroborated. Photographs should not routinely be taken for intelligence purposes, as this is governed by the Regulation of Investigatory Powers Act (RIPA) 2000.

18.3 The mobile devices should not be used to replace all Crime Scene Investigation (CSI) photography. CSI should be called where:

- Photographs are being taken for serious or major crime;
- Extensive or large numbers of photographs are required;
- When evidential comparison will be required (e.g. footwear-marks);
- Where photographs taken using the mobile devices is not fit for purpose.

18.4 Use of the devices for CSI photography purposes is permitted in instances where waiting for CSI would lead to a loss of evidence (e.g. an item in situ which will have to be seized or moved).

18.5 Images captured using a mobile device must be uploaded to the appropriate system or networked storage at the first available opportunity. Once the digital asset has been successfully uploaded, the original image should be deleted from the mobile device.

19. Prohibited Activities

19.1 The following activities are strictly prohibited in relation to the use of Force devices:

Official

Version Number: 3

Page 9 of 12

MOBILE DEVICE USE POLICY

Official

- Illegal, fraudulent or malicious activities;
- Activities for the purposes of personal or commercial financial gain;
- Solicitation of businesses or services;
- Harassing another person by way of uninvited email, text messages or calls;
- The use of lewd or offensive language in emails, text messages or calls;
- Displaying, storing, downloading and distribution of offensive, obscene, racist or sexist material other than for policing purposes;
- Storing any information on the device not connected to the user's role within Norfolk or Suffolk Constabularies without the written permission of the Force Information Security officer;
- Accessing the device with another user's account details;
- Allowing access by an unauthorised user to information which is stored or can be viewed on the device and accessed via the secure network;
- Use of personal social media accounts or to take personal and non-operational photographs/recordings/videos.

20. Monitoring

- 20.1 The contents of the Constabularies' systems and data are the Constabularies' property. This includes all materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a Constabulary device (collectively referred to as "content").
- 20.2 The Constabularies' reserve the right to monitor, intercept, review and erase, without further notice, all content on a Constabulary device. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device as well as keystroke capturing and other network monitoring technologies, whether or not the device is in a user's possession.
- 20.3 It is possible that personal data on a Constabulary device may be inadvertently monitored, intercepted, reviewed or erased. Therefore, users should have no expectation of privacy in any data on the device. Users are advised not to use Constabulary systems for any matter intended to be kept private or confidential. If users use a device to process personal data about third parties (for example, family and friends), they should be aware that this may be inadvertently monitored, intercepted, reviewed or erased.
- 20.4 Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for the Constabularies' to comply with a legal obligation or for legitimate business purposes, including, without limitation, in order to:

MOBILE DEVICE USE POLICY

Official

- Prevent misuse of the device and protect the Constabularies' data;
- Ensure compliance with the Constabularies' rules, standards of conduct and policies in force from time to time (including this policy);
- Monitor performance at work; and
- Ensure that users do not use the Constabularies' facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

20.5 The Constabularies' may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. The Constabularies' may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.

20.6 By using the device, users acknowledge that the Constabularies are entitled to conduct such monitoring where they have a legitimate basis to do so, and confirm agreement (without further notice or permission) to the Constabularies' right to copy, erase or remotely wipe the entire device (including any personal data stored on the device).

21. Personal Data

21.1 The Constabularies have a legitimate basis on which to access and protect Constabulary data stored or processed on a device, including the content of any communications sent or received from the device. However, the Constabularies recognise the need to balance their obligation to process data for legitimate purposes, with a user's expectations of privacy in respect of their personal data. Therefore, when taking (or considering taking) action to access a device or delete data on a device (remotely or otherwise) in accordance with this policy, the Constabularies will, where practicable:

- Consider whether the action is proportionate in light of the potential damage to the Constabularies, our staff/officers or the public;
- Consider if there is an alternative method of dealing with the potential risks to the Constabularies' interests (recognising that such decisions often require urgent action);
- Take reasonable steps to minimise loss of a user's personal data on a device, although the Constabularies shall not be responsible for any such loss that may occur; and
- Delete any such personal data that has been copied as soon as it comes to the Constabularies' attention (provided it is not personal data which is also Constabulary data, including all personal e-mails sent or received using the Constabularies' email system).

21.2 To reduce the likelihood of the Constabularies' inadvertently accessing a user's personal data, or the personal data of third parties, users must comply with the following steps to separate Constabulary data from their personal data on the device:

Official

Version Number: 3

Page 11 of 12

MOBILE DEVICE USE POLICY

Official

- Organise files within the device specifically into designated folders that clearly distinguish between Constabulary data and personal data (for example, marking your own folders as "PERSONAL");
- Do not use work e-mail for personal purposes;
- Do not store third party personal data (e.g. in relation to family and friends) on the device;
- Regularly backup all personal data stored on the device.

22. Device Management, Transfer and Return

22.1 If the device is not used for any length of time, ICT may decide that it should be transferred to another user or returned to ICT.

22.2 In the event of the user no longer working for Norfolk or Suffolk Constabularies, the device(s) and all equipment issued with it must be returned prior to the user's last working day.

22.3 A device(s) and all equipment issued with it must be returned in accordance with paragraph 20.2 when the user is taking maternity leave, adoption leave, shared parental leave, a career break, is on secondment or has been suspended, unless the associated policy allows for the device and ICT account to remain active through an appropriate approval process. Please refer to the relevant policy e.g. Maternity Leave, Disciplinary, Misconduct etc.

22.4 If a user is moving to a role which does not qualify for a personal issue device on a permanent basis, or a temporary basis beyond 12 months, the device(s) and all equipment issued with it should be returned to ICT Customer Contact prior to the move.

22.5 The devices remain the property of Norfolk and Suffolk Constabularies and may be withdrawn at any time.

22.6