POLICY

MOBILE DEVICE USE POLICY

Policy owners	Director of ICT
Policy holder	Director of ICT
Author	James Nobbs

Approved by

Legal Services	N/A
Policy owner	12 September 2017
JJNCC	7 September 2017

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication date	12 September 2017
Review date	12 September 2020
APP Checked	Yes
College of Policing Code of Ethics	Yes

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation/Law specific to the subject of this policy document

Act (title and year)

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

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
Health & Safety Legislation
General Data Protection Regulation (GDPR) and Data Protection Act 2018
Freedom Of Information Act 2000

Other Related Documents

- Social Media Policy
- Provision of ICT Equipment
- College of Policing Code of Ethics
- Standards of Professional Behaviour for Officers and Staff

1. Introduction

1.1 The purpose of the policy is to provide users of mobile devices 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 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 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. Device Deployment

2.1 The purpose of the deployment of mobile devices across Norfolk and Suffolk is:

- 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 and to work in a smarter and more cost effective way.

3. User Responsibilities

3.1 Users should follow these procedures at all times while operating their device. Failure to comply with these procedures may result in disciplinary proceedings being carried out.

3.2 All users must read, fully understand and accept the procedures and advice in this document. Before using their device, staff will be required to sign a Terms and Conditions document.

3.3 Users are responsible for the physical security of their device, and 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.

3.4 When using a 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.

3.5 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 open offices, hotel rooms, or on view at home, etc.

3.6 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.

3.7 It is an individual'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.

3.8 Users must not attempt to run unsigned code (e.g. jailbreak) 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.

4. Incident Response

4.1 If the 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.

4.2 Reports of this type of incident should be done immediately and prior to a protracted search.

4.3 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.

4.4 If users believe that their password has been compromised it must be changed immediately.

4.5 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.

4.6 If the device stops functioning as normal, users should 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. Officers must not tamper or dismantle any issued device.

4.7 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.

4.8 Hardware issues, for example cracked screens or broken cases, should be reported to the ICT Service Desk in the first instance.

5. Mobile Working Expectations

5.1 There is no expectation or work related requirement for users to use any devices whilst off duty.

5.2 The devices will allow 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.

5.3 Officers and police staff *will not* be classed as being on duty if they do check emails or carry out other administrative task, unless the need to do so is necessary as part of a live incident and not for their personal interest.

5.4 In addition to the above, there is no expectation for officers or police staff to have any devices *accessible* off duty unless as required for on-call duties.

5.5 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.

6. Passwords

6.1 It is important that a strong password is chosen, 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.

6.2 Unless advised otherwise, passwords must meet the following requirements:

- It must contain a mixture of upper 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.

6.3 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.

6.4 This password requirement will be enforced by the Mobile Device Manager.

6.5 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.

6.6 For security purposes, after 10 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.

6.7 Further information on the Constabularies' Password Policy can be found within the Acceptable Use of Information Systems and Assets Policy.

7. Voicemail

7.1 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.

7.2 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.

7.3 Messages left should be considered private and should not be accessed without the permission of the 'owner' of the voicemail facility or the nominated Force Telecoms Manager.

7.4 Voicemail greeting messages should be updated regularly, especially for periods of extended absence. Additionally, alternative contacts should be provided where possible.

7.5 Voicemail messages should be checked as soon as possible after returning from a period of leave.

7.6 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.

8. Wi-Fi

8.1 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.

8.2 ICT security protocols will block any unsafe connections. Connection to private internet hubs is permitted when permission is given.

9. Bluetooth

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

10. Social Media

10.1 Access to social media such as Twitter and Facebook will be possible from the devices for users to log into official Norfolk and Suffolk Constabulary accounts, if authorised. The existing Digital and Social Media policy should be referenced for terms of use.

10.2 Personal social media accounts must not be used via a device issued for work use.

11. Email

11.1 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.

11.2 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.

11.3 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.

11.4 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.

12. Internet Use

12.1 The devices will allow access to the Internet and users will be subject to the same level of moderating, supervision and web marshalling as with normal desktop use.

12.2 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.

13. Applications / Services

13.1 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.

13.2 If an app is identified as beneficial, then this should be requested via the ICT Service Desk for further assessment and consideration.

13.3 Users will be notified whether an application has been approved or declined once a decision has been made.

14. Digital Images

14.1 Police officers and staff must use the 'National Decision Making Model' (NDMM) to decide when and in what circumstances to capture a Digital Image. This will only ever be for a legitimate policing purpose.

14.2 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.

14.3 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.

14.4 Though use of the devices 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).

15. Prohibited Activities

15.1 The following activities are strictly prohibited:

- 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.

16. Device management, transfer or disposal

16.1 If the device is not used for any length of time, ICT may make arrangements for it to be transferred to another user.

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

16.3 This also includes when the user is taking maternity leave, a career break, is on secondment or has been suspended. If moving to a role which does not qualify for a personal issue device on a permanent or temporary basis beyond 12 months, the devices and associated accessories should be returned to ICT Customer Contact.

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