Smart Phone and Mobile Data Device Policy
North Wales Police

Smart Phone and Mobile Data Device Policy

Governance: People & Resources Committee
Policy Owner: Chief Information Officer
Department: Corporate Services
Policy Writer: Chief Information Officer
Policy Number: 080 Version: 2.1
Effective Date: 23/10/2017
Review Date: 23/10/2019

<table>
<thead>
<tr>
<th>Version No</th>
<th>Author</th>
<th>Changes</th>
<th>Ratification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Ian Davies, CIO</td>
<td>Complete review to bring in line with new policy standards. Removal of personal use.</td>
<td>People &amp; Resources Committee</td>
</tr>
<tr>
<td>2.1</td>
<td>Tom King, SMT / ICT Administrator</td>
<td>Grammatical corrections</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Contents

1. WHY IS THIS POLICY REQUIRED? ........................................................................................................ 2
2. WHO SHOULD USE THIS POLICY? ........................................................................................................ 2
3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY? .............................................................. 2
4. THE PROCESS .................................................................................................................................. 2
   4.1 CONDUCT .......................................................................................................................... 2
   4.2 BUSINESS AND PERSONAL USE ......................................................................................... 3
   4.3 SECURITY .......................................................................................................................... 4
   4.4 ASSET CONTROL ................................................................................................................ 6
   4.5 MONITORING ..................................................................................................................... 6
   4.6 TELEPHONE FUNCTION ..................................................................................................... 7
   4.7 MOBILE DEVICE CAMERA FUNCTION .............................................................................. 7
   4.8 USE OF EMAIL, INTRANET AND INTERNET ..................................................................... 7
   4.9 HARDWARE & SOFTWARE ................................................................................................. 8
   4.10 OPERATIONAL USE ........................................................................................................... 9
   4.11 HEALTH & SAFETY ......................................................................................................... 9
   4.12 DRIVING ......................................................................................................................... 9
   4.13 SUPPORT ....................................................................................................................... 9
   4.14 MAINTENANCE ............................................................................................................... 9
   4.15 SERVICE AVAILABILITY .............................................................................................. 10
5. DECLARATION & LEGALITIES ......................................................................................................... 10

APPENDIX A – BUSINESS & LIMITED PERSONAL USE REQUEST FORM ......................... 11
1. WHY IS THIS POLICY REQUIRED?

This policy will:

1.1 Provide guidance to NWP personnel in the use of smart phones and mobile data devices.

1.2 Set out mandatory actions required by users.

2. WHO SHOULD USE THIS POLICY?

2.1 This policy should be used by all NWP personnel, referred to as ‘users’ throughout this policy who have been issued with a smart phone or mobile data device referred to as ‘devices’ or ‘equipment’ throughout this policy.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

3.1 This policy should be read in conjunction with the following documents:

- Force Information Standards Policy (FISP) and its associated Procedures
- NWP Email and Network Drive Procedure
- NWP Internet Procedure
- Force Imaging (Photography) Policy
- Force Imaging (Video) Policy
- Information Security Incident Procedure

4. THE PROCESS

4.1 CONDUCT

Users of force devices must abide at all times to standards of professional behaviour as defined by the Police Conduct Regulations 2008 for Officers and Police Staff Conditions of Service for Staff. In particular users of NWP Force devices must not use them for the following purposes:

a) To communicate information that may disparage, threaten, or harass others.

b) To make statements that may be considered defamatory.

c) To communicate sexually explicit material, propositions or suggestive remarks.

d) To communicate aggressive material including threats, violence, abuse, obscenities or material that promotes illegal acts.

e) To discriminate in any way, to harass or victimise including insults or “jokes” related to a person’s protected characteristic (e.g. age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation).

f) To conduct political, religious or any other inappropriate lobbying or canvassing, excluding Trade Union, Police Association or Staff Association.

g) To conduct personal, private or freelance business interests.
4.1.1 Legislation

Users must comply with all relevant force policies including the Force Information Standards Policy, the email, internet appendices & all relevant policies that refer to any application available via a mobile device.

Users should also ensure that all use of the devices is in accordance with the provisions of the Data Protection Act 1988 and the Computer Misuse Act 1990.

Users of devices should be aware that transactions undertaken will be audited from time to time and any breach of any policies or legislation may result in disciplinary action.

The account of any user found to have contravened any policy or legislation may be suspended or withdrawn pending investigation, and notification passed to the Force Professional Standards Department.

4.1.2 Misuse of Devices

It will be the responsibility of all Police Officers and Police Staff to adhere to this policy.

Any user in breach of this policy may be liable to have access suspected or withdrawn. Non-compliance with this policy may result in disciplinary findings of misconduct or gross misconduct procedures which could lead to loss of employment and / or criminal proceedings.

4.2 BUSINESS AND PERSONAL USE

The issue of a force Smart Phones & Mobile Data device is for BUSINESS use only. All usage of the device must be for a valid policing purpose.

No PERSONAL use must be made of the device, including calls, text messages or data usage, whilst either on or off duty.

It is accepted that on rare occasions emergency personal calls need to be made to update partners/family/etc. about being retained on duty/duty changes or other such work related matters. In such cases these will be accepted as ‘work related’.

No device may be used for any personal purpose and no personal information outside the policing remit may be stored on any such device.

Devices may be, if desired, taken home by the user for safekeeping, checking of emails (e.g. overtime offers) or checking of duty rostering for example. The device will not be used to retrieve or submit data from Force systems whilst off duty unless there are exceptional operational circumstances and the user is fit for duty.

Devices must not be taken outside of the UK without approval from the Chief Information Officer.

The definition of a private call/text is deemed as a call/text made not in relation to the delivery or support of policing.
It is accepted that there are certain specialist operational roles within the Force which require the user to be contactable, even if they are not formally on duty or on call. In order to facilitate these users to potentially be contactable, the specialist roles can (if they wish) apply for a classification of “Business & Limited Personal User”, in order to increase the likelihood of being contactable whilst off duty.

NWP Employees who wish to apply must:

- Complete the form included in Appendix A
- Indicate the criteria to which applies for their NWP role
- Obtain approval from their SMT
- Submit completed Appendix A to the Shared Services Facility (SSF) Finance Payroll & Pensions for processing once approved.

A fixed fee will be deducted from these specialist users’ salaries after tax until such time SSF Finance Payroll & Pensions is informed otherwise.

A Business & Limited Personal User is permitted to use the device for limited personal calls, text messages and use limited mobile data functionality.

Frequency of personal use whilst on duty must be kept to a minimum and should not impact in any way your ability to effectively and efficiently undertake your role.

Billing and monthly use will continue to be examined monthly by Finance & Resources to monitor excessive, inappropriate and fair use of their connection.

Business and Limited Personal users can request (via SSF) sight of their monthly usage to ascertain an appropriate level of personal usage.

The following limitations on personal use apply on all devices:

- Personal calls should normally be made solely to UK geographic and mobile (07) numbers only. Exceptionally, calls may be made to non-geographic (08) numbers
- Devices must not be taken outside of the UK without approval from the Chief Information Officer.
- It is recommended that mobile data is turned off when not within the UK. Care should be taken to avoid excessive voice and data roaming charges when using the device abroad.
- Personal calls to premium-rate (09) and international numbers should be avoided given the high costs of such calls and the capped personal allowance. The same would apply to premium rate text messages.

4.3 SECURITY

All devices are to be used for non-sensitive voice conversations only, unless there is an exceptional operational requirement to do so which must be dynamically risk assessed. Users should be aware of being overlooked or overheard (shoulder-surfing or eavesdropping) and/or loss or theft.

Staff should protect their device using a secure password or PIN.
4.3.1 Physical Security

The user is fully responsible for the physical security of the device at all times.

The secure handling of any device issued to NWP staff is the user’s responsibility.

Every effort must be made to ensure that no unauthorised person gains access to the device or data held thereon. This includes leaving the device in a Police vehicle.

Each device will be allocated on a ‘personal issue’ basis. The device will only work when the valid password of the assigned user is entered. The devices cannot and must not be shared or provided to another NWP user.

Access to apps on the device may require a secondary password to be entered.

Bluetooth is not a secure connection; use of Bluetooth should be avoided but if operationally necessary it must be used in accordance with the guidance issued by Information Standards & Compliance Department.

4.3.2 Security of Data

Users should ensure that they keep their passwords and PIN numbers secure and do not disclose them to other users.

The user will ensure that, in addition to any measures listed in this document, all usage of the equipment, and any data stored therein, fully complies with the Data Protection Act 1998 and the Computer Misuse Act 1990.

The user is responsible for ensuring the security of any data whilst on the device.

Disclosure of any data from the device to any third party should only be undertaken in accordance with Force policy and with the consent of the data owner, via the Force Chief Information Officer (CIO).

Data above the Government Security Classification (GSC) ‘OFFICIAL’ level will not be stored on, downloaded to, sent to or from the device.

The user must make every effort to ensure that no unauthorised persons gain access to the equipment or data at any time. This includes the screen being viewed by any unauthorised person.

4.3.3 Security Incident Reporting

If a user believes their device has been lost or stolen, or for any reason cannot account for its whereabouts, they must contact the ICT service desk immediately (contacts below) to have the device disabled (stunned or killed). The helpdesk will take note of the details and take the appropriate action to disable the device. It is also advisable that the user report the loss/theft to the Force Call-handling Centre – via the police priority number as soon as possible.

The loss/theft must also be reported to Information Standards & Compliance Section (contact below) to advise them as soon as possible following contact with the service desk.
Other security incidents which should be reported to Information Standards & Compliance include the unavailability of data, suspected tampering or unauthorised disclosure of data, whether accidental or not. See the Information Security Incident Procedure (part of the Force Information Standards Policy) for further information.

To report loss or theft of mobile device:
• Internal Ext 4100 or External 03332 079992
• Email: nwpictservicedesk.uk@cgi.com

Information Standards & Compliance reporting:
• Internal Ext 05399 or External 01492 05399
• Email: Information Security Incidents

4.4 ASSET CONTROL

All procurement of devices will be centrally controlled and authorised by the Force IT Department. Once issued, the end user will be responsible for the device.

All devices will remain the property of North Wales Police and there should be no expectation of privacy. Devices could be subject of routine examination.

Any issues or faults with the device should be raised via the ICT service desk on ext. 4100.

If the device is no longer required then it should be returned to the IT Department for reallocation or secure disposal.

Users must hand in their device to their line manager on their last day of work as per the HR leavers check list. Failure to do so may incur equipment charges via the users final pay slip.

4.5 MONITORING

The mobile service provider can automatically generate reports which identify devices exhibiting excessively high monthly usage of voice or data. These reports are routinely examined by Finance and Resources to verify the appropriateness of individual usage patterns and will take whatever action may be appropriate in specific circumstances.

Any consistent misuse will be referred to Professional Standards Department for their consideration of any further action.

Audit and monitoring of use will be undertaken for security and integrity purposes. There should be no expectation of privacy.

Covert monitoring will only be used where the level of intrusion will be proportionate to the issue being investigated and/or evaluated for compliance with Force standards. Authorisation will be in accordance with Force Policy and should comply with RIPA legislation which should also ensure compliance with other relevant legislation e.g. the Data Protection Act 1998 and the Human Rights Act 1998.

ICT and Professional Standards Departments may monitor user activity for security and evaluation reasons whilst devices are connected to North Wales Police systems; this
could include such items as systems accessed, duration of connection, failed access attempts etc.

4.6 TELEPHONE FUNCTION

Users should not have a personal voice mail greeting which could cause offence to any member of the public or a colleague. It should specify only who the caller has reached and explain where/who to contact within NWP in the event of something urgent.

Premium rate numbers including commercial directory enquiry numbers must not be called from the device unless there is a pressing operational need. Any such usage must be recorded in a pocket book and/or e-mailed to a supervisor. Any premium rate numbers dialled will be picked up as part of the monthly billing review and any calls that cannot be specifically accounted for as per the above will be considered as a potential misconduct/disciplinary matter.

Users should not send any messages to any Premium Rate text message services such as promotional offers or those associated with Television shows.

Users must not subscribe to any chargeable SMS text message alert mechanisms that result in text messages being received by the device. Any such texts sent will be picked up as part of the monthly billing review and will be considered as a potential misconduct/disciplinary matter.

Users are actively encouraged to use the device to its full potential for NWP operational and business purposes.

4.7 MOBILE DEVICE CAMERA FUNCTION

The camera function is only to be used for work purposes and not to be used for any personal reasons.

The taking of evidential photographs or video using the device camera must follow the guidance as set out in the Force Imaging (photography) Policy and Imaging (video) Policy. Evidential images and videos must not be sent or downloaded from the device by any means other than that set out in said Policies. Evidential images and video must be deleted following successful transmission to the imaging department.

Photographs, video footage and audio recordings should only be taken when the lawful power to take them is present. Users should be aware of general Regulation of Investigatory Powers Act (RIPA) issues, surveillance policy, human rights & data protection legislation.

4.8 USE OF EMAIL, INTRANET AND INTERNET

4.8.1 Email

Users will have access to their Force email account via the device.

Email may only be used for work-related purposes.

Users should be aware that, when sending or receiving email, no “OFFICIAL” police information may be sent to any non-police address or insecure email account.
No information graded above ‘OFFICIAL’ may be sent via the devices to any email account (e.g. SECRET OR TOP SECRET).

4.8.2 Internet and Intranet

Users will be able to access the NWP Intranet from the device. This will include SharePoint sites and the HR Self Service portal.

Users will have access to the Internet from the device. The Intranet and Internet should only be accessed for work-related purposes.

4.8.3 Access to Force Systems

Users will have access to some Force systems via the “mobile app” on the device.

Before being allowed access via the device to any data held on any system, the user must have successfully completed appropriate training in the operating procedures and security issues relevant to each application the user needs to access.

All relevant legislation, NWP policies and procedures for access and use of information will apply to accessing Force systems via the device: these include the successful completion of mandatory training prior to the granting of access rights by the system administrator and the accessing of information for policing purposes only.

**Under no circumstances will Police data be accessed for private or personal reasons**

The device will not be used to retrieve or submit data from Force systems whilst off duty unless there are exceptional operational circumstances and the user is fit for duty.

4.8.4 Access to Consumer Apps

Users will have access to a selection of consumer apps approved by the Force to be used for a work related purpose.

The approved consumer apps are to be used for a policing purpose only and should not be used for personal accounts.

For further guidance on use of social media apps, please refer to the Online Social Networking policy.

4.9 HARDWARE & SOFTWARE

In relation to voice use on the device, users should take account that the device does not encrypt voice communications.

When supplied, the device will be installed with software approved by the Force. No additional software will be used or installed unless approved by the ICT Department.

When supplied, the equipment will have been configured by the ICT Department. The configuration may allow the user to personalise certain items on the device. The user will not attempt to re-configure any other items that may affect the operating system or functionality of the device unless prior approval has been given by the ICT Department.
No connection between a mobile device and any other computer/communications equipment or storage device other than that owned and supplied by North Wales Police will be permitted.

4.10 OPERATIONAL USE

Sometimes users may need to turn the device off. Users should follow the same procedures when using any other police equipment (for example Breath Test, speed detection) – as per the force guidance for that police equipment.

4.11 HEALTH & SAFETY

The device should be holstered in the case provided when not in use. Only use the device in places and at times where the use of a Mobile Data device is permitted and when it is safe to do so.

4.12 DRIVING

The Road Vehicles (Construction and Use) (Amendment) (No 4) Regulations 2003 strictly prohibited the use of handheld mobile phones, or similar devices, while driving any motor vehicle (including a motorcycle) on a road.

In line with Police Use of Vehicle and Management Risk Policy, Drivers may use hands-free equipment that has been installed by Fleet Services for receiving calls only. Use must be kept to an absolute minimum so that full control of the vehicle is maintained at all times. Even though use as above may be legal, drivers should be aware that the higher the speed they are travelling and the more distracting the task they are engaged in, the greater the risk in their use. Hence, wherever possible, drivers should stop whilst using the equipment.

4.13 SUPPORT

Support is provided 24/7 via the channels below:

- ICT Helpdesk
- Internal Ext 4100 or External 03332 079992
- Email: nwpictservicedesk.uk@cgi.com

Examples of assistance the helpdesk can assist with include:

- Re-setting passcodes
- General issues & training guidance
- Taking reports of lost and/or stolen devices in order to Stun / Kill disable the device
- Access to the NWP App
- Broken or faulty devices
- All calls to the service desk from users will be logged and recorded for training purposes

4.14 MAINTENANCE

The device requires little maintenance, and basic cleaning of the screen/unit can be performed by the user.
Users are responsible for ensuring that their device is regularly charged and that it is in full working order when required for duty.

If the device becomes faulty, the user should report this to the ICT service desk.

ICT will regularly review logs of usage statistics to determine systems loadings, peak access times etc. This will allow early identification of potential problems.

4.15 SERVICE AVAILABILITY

The ICT department aim to make device access to the relevant NWP systems available 100% of the time to authorised users; however the following exceptions should be noted:

- Scheduled Maintenance downtime.
- Other circumstances beyond NWP’s reasonable control.

It should be noted that whilst availability will be maintained as much as possible, there is no guarantee of performance over the public mobile networks, including coverage.

5. DECLARATION & LEGALITIES

5.1 In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall the intention of this policy is to provide a safer North Wales.

5.2 In the writing of this policy cognisance has been taken of the College of Policing Code of Ethics (2014).

5.3 North Wales Police policies will be written in accordance with the approved corporate format and published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force Publication Scheme and Freedom of Information Act 2000.

5.4 The following main legal requirements have been identified within this policy:
- Equality Act 2010
- Human Rights Act 1998
- Welsh Language Act 1993 and the NWP Welsh Language Scheme
- Data Protection Act 1998
- Freedom of Information Act 2000
- Health and Safety Act 1974

5.5 This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).

5.6 New legislative requirements or changes in Force structure may necessitate a review of this policy document.
APPENDIX A – BUSINESS & LIMITED PERSONAL USE REQUEST FORM

BUSINESS & LIMITED PERSONAL USE REQUEST

DATE: 

NAME: 

COLLAR / PAY NUMBER : 

TO:  SSF Finance Payroll & Pensions, Colwyn Bay

I wish to change my mobile phone usage to Business & Limited Personal Use.

I authorise SSF Finance Payroll & Pensions to deduct £2.75 per month from my salary after tax until I inform them otherwise.

The criteria for my limited personal use is indicated below (indicate all that apply)

Information Asset Owner for a critical force system (e.g. RMS, iCAD etc) □

Responsible for large number of Employees (e.g. Department or more) □

Specialist operational knowledge, skills or other rational (specify below) □

Deductions should begin on month/year: 

Mobile Phone Number: 

☐ I certify that I have read and understood the Mobile/Smart Phone Policy and agree to abide by it

Signed by:  
(Holder of Phone)

Name of Holder (BLOCK CAPITALS): 

Certified by: 
HEAD OF POLICING FUNCTION

Date: 

North Wales Police – Corporate Services