



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

MOBILE PHONE POLICY

Governance:	Senior Leadership Team		
Document Type:	Policy		
Policy Owner:	Director of Finance and Resources		
Department:	ICT / Chief Information Office		
Policy Writer:	Chief Information Officer – Ian Davies		
Policy Number:	080	Version:	3.0
Effective Date:	25/05/20		
Recommended Review Date:	25/05/22		

POLICY

CHANGE HISTORY			
Version No	Author	Changes	Ratification
2.0	Ian Davies, CIO	Complete review to bring in line with new policy standards. Removal of personal use.	People & Resources Committee
2.1	SMT / ICT Administrator	Grammatical corrections	N/A
2.2	Ian Davies, CIO	Section 4.5 para 3 amended	ACU advise
3.0	FP&G Officer	Transferred to new template and reviewed to bring in line with policy standards	

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
4.1.1 Legislation	2
4.1.2 Misuse of Devices	3
4.2 BUSINESS AND PERSONAL USE	3
4.3 SECURITY	4
4.3.1 Physical Security	4
4.3.2 Security of Data	4
4.3.3 Security Incident Reporting	5
4.4 ASSET CONTROL.....	5
4.5 MONITORING.....	6
4.6 TELEPHONE FUNCTION.....	6
4.7 EMAIL, INTRANET AND INTERNET FUNCTION	6
4.7.1 Email.....	6
4.7.2 Internet and Intranet.....	7
4.7.3 Access to Force Systems	7
4.7.4 Access to Consumer Apps.....	7
4.8 HARDWARE AND SOFTWARE	7
4.9 HEALTH AND SAFETY	8
4.9.1 Driving	8
4.10 SUPPORT	8
4.11 MAINTENANCE	8
4.12 SERVICE AVAILABILITY	8
5. DECLARATION & LEGALITIES.....	9
6. APPENDIX A – BUSINESS & LIMITED PERSONAL USE REQUEST FORM	9

1. WHY IS THIS POLICY REQUIRED?

This policy will

- 1.1 Provide guidance to NWP officers and staff 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 officers and staff, referred to as 'users' throughout this policy, who have been issued with a smart phone or mobile data device referred to as 'devices' throughout this policy.

3. WHAT SHOULD I CONSIDER WHEN USING THIS POLICY?

- 3.1 This policy should be read in conjunction with the Force Information Standards Policy.

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 2020 for Officers and Police Staff Conditions of Service for Staff. In particular users must not use the devices for the following purposes:

- a) To communicate information that may ridicule, threaten, or harass others.
- b) To make statements that may be considered offensive.
- 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, marriage and civil partnership, pregnancy and maternity, race and ethnicity, religion or belief, sex and sexual orientation).
- f) To conduct political, religious or any other inappropriate promoting or campaigning, excluding Trade Union, Police Association or Staff Association.
- g) To conduct personal, private or freelance business interests.

4.1.1 Legislation

Users should ensure that all use of the device is in accordance with the provisions of the **Data Protection Act 2018** and the **Computer Misuse Act 1990**.

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

The account of any user found to have breached 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 is the responsibility of all users to adhere to this policy.

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

4.2 **BUSINESS AND PERSONAL USE**

The issue of a device is for BUSINESS use only. All usage 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.

The definition of a private call/text is deemed as a call/text made not in relation to a policing purpose.

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'.

Devices may be, if desired, taken home by users 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 fit for duty.

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

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 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
- Obtain approval from their SMT
- Submit the completed and approved Appendix A to the Shared Services Facility (SSF) Finance Payroll & Pensions for processing (SSFPayroll@nthwales.pnn.police.uk).

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 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 will continue to be examined monthly by Finance & Resources to monitor excessive, inappropriate and fair use of the 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. Calls may be made to non-geographic (08) numbers in exceptional circumstances.
- 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 applies to premium rate text messages.

4.3 SECURITY

All devices should be used for non-sensitive voice conversations only, text messaging should be avoided 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 and handling of the device at all times.

Every effort must be made to ensure that no unauthorised person gains access to the device or data therein. 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. 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 and therefore 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 take account that the device does not encrypt voice communications. It's therefore imperative that users must keep their passwords and PIN numbers secure and not disclose them to other users.

Users must ensure that, in addition to measures listed in this document, all usage of the devices, and any data stored therein, must fully comply with the Data Protection Act 2018 and the Computer Misuse Act 1990.

Users are 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).

4.3.3 Security Incident Reporting

If a user believes their device has been lost or stolen, or for any reason they cannot account for its whereabouts, they must contact the ICT service desk (contact details below) immediately. The helpdesk will take note of the details and take the appropriate action to disable the device. It is also advisable that the user reports the loss/theft to the FCC.

ICT Service Desk Contact Details

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

The loss/theft must also be reported to the Information Standards & Compliance department (contact details below) as soon as possible following contact with the service desk.

Information Standards & Compliance Department Contact Details:

- Internal Ext 05399 or External 01492 05399
- Email: infostandandcompliance@nthwales.pnn.police.uk

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. Refer to the [Information Security Incident Procedure](#) for further information.

4.4 ASSET CONTROL

All procurement of devices will be centrally controlled and authorised by the Force ICT Department. Once issued, the 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 extension 4100 or by calling 03332 079992.

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

Users must return 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 charges via the users final pay slip.

4.5 MONITORING

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

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

Audit and monitoring of devices, whether for Business or Personal use, will be undertaken for security and integrity purposes. There should be no expectation of privacy by either Business only or Business and Limited Personal Users. It is possible to monitor the location of the device and to read/recover the content of emails and texts remotely.

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 RIPA legislation which will also ensure compliance with other relevant legislation e.g. the Data Protection Act 2018 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 colleagues. 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 will be considered as a potential misconduct/disciplinary matter.

Users should not send any messages to any Premium Rate text message services. 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 EMAIL, INTRANET AND INTERNET FUNCTION

4.7.1 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).

4.7.2 Internet and Intranet

Users will be able to access the NWP Intranet site from the device. This will include SharePoint sites and the HR Self Service portal. Access instructions are detailed in appendix b.

Users will have access to the Internet from the device, however it should only be accessed for work-related purposes.

4.7.3 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.

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 should 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.

4.7.4 Access to Consumer Apps

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

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

4.8 HARDWARE AND SOFTWARE

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 a user to personalise certain items on the device. The user must 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.

4.9 HEALTH AND SAFETY

The device should be holstered in the protective case provided and the screen protector provided should be affixed to the device prior to use..

Only use the device in places and at times where the use of Mobile Data devices is permitted and when it is safe to do so.

4.9.1 Driving

The Road Vehicles (Construction and Use) (Amendment) (No 4) Regulations 2003 strictly prohibits 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. However use must be kept to an absolute minimum so that full control of the vehicle is maintained at all times.

4.10 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 disable the device
- Access to the NWP Apps
- Broken or faulty devices

All calls to the service desk from users will be logged and recorded for training purposes

4.11 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.

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

4.12 SERVICE AVAILABILITY

The ICT department aim to make access to the relevant NWP systems available 100% of the time; 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 make North Wales the safest place in the UK.
- 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
 - The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
 - Data Protection Act 2018
 - 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.

6. 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: _____