

REFERENCE NUMBER OF DOCUMENT:	11.2.378.01
COMMITTEE IDENTIFICATION:	Galago Directors
SECRETARIAT:	MS
DOCUMENT TYPE:	External Policy
DOCUMENT LANGUAGE:	E
THIS POLICY IS FOR:	Staff including Agency Workers (temporary workers), Commissioners and Service Users

MOBILE PHONE & PORTABLE DEVICE USE

WARNING:

If the document contains proprietary information, it may only be released to third parties after management has approved its release.

Unless otherwise marked, documents are uncontrolled; uncontrolled documents are not subject to update notifications.

The latest revision of this document can be found in the reference panel above. It can also be determined and double checked by checking the 'Master Document List' before using or sending.

Any changes must be requested through the 'Document Control Manager' by submitting a 'Document Change Request' form.

MOBILE PHONE AND PORTABLE DEVICE USE POLICY AND PROCEDURE

POLICY AIM

The purpose of this policy is to set clear expectations for the safe and professional use of personal mobile phones by staff including Agency Workers when supporting service users in the community.

Nursing Direct does not provide work mobile phones; therefore, staff including Agency Workers use their own devices to access the OneTouch App to record care notes and other relevant information. This policy ensures mobile phone use supports safe, effective care while protecting the privacy, dignity, and confidentiality of service users in line with data protection requirements and organisational standards.

This policy applies to all staff including Agency Workers delivering care in community settings and does not apply to those based in the Nursing Direct head office. Personal calls, texts, and messaging are not permitted during working hours, except in exceptional circumstances. Where a personal phone is used for work purposes, staff including Agency Workers must follow this policy as if using a business device, keep all service user information secure and confidential, and understand they remain responsible for the loss, theft, or damage of their own device.

1. PURPOSE

1.1 To detail the effective and safe use and management of mobile phones and portable devices being used for work purposes by staff including Agency Workers at Nursing Direct.

1.2 The term portable device for the purpose of this policy covers items such as:

- Laptops
- Tablets
- Smart Watches
- Photo and Video Cameras
- Sat Nav
- Sim Cards
- USB Devices
- Smart Phones
- Power Banks

As well as any other device that may be defined as a portable electronic device.

1.3 To support Nursing Direct in meeting the Care Quality Commission (CQC) Key Lines of Enquiry (KLOEs) and Quality Statements to comply with legislation, regulation, and best practice standards.

1.4 RELEVANT LEGISLATION

- The Care Act 2014
- Health and Social Care Act 2008 (Registration and Regulated Activities) (Amendment) Regulations 2015
- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999
- Data Protection Act 2018
- UK GDPR
- Corporate Manslaughter and Corporate Homicide Act 2007
- Data (Use and Access) Act 2025

2. SCOPE

2.1 Roles Affected:

- All staff including Agency Workers

2.2 People Affected:

- Service Users

2.3 Stakeholders Affected:

- Family Commissioners

3. OBJECTIVES

3.1 The risk of accidental, unauthorised, or inappropriate use of mobile phones and portable devices is eliminated or reduced and there is full compliance with legislation with regard to the security and safety of the mobile phone and portable device.

3.2 Staff including Agency Workers have a working knowledge of their responsibilities in relation to the use of personal mobiles and portable devices for work related activity.

4. POLICY

4.1 Nursing Direct believes that effective communication systems are vital for a successful service. Mobile phones and some portable devices support robust communication channels.

Nursing Direct ensures that all mobile and portable device use complies with the UK GDPR, Data Protection Act 2018 and the Data (Use and Access) Act 2025. Staff including Agency Workers must use devices in a manner that maintains confidentiality, integrity, and security of information at all times.

4.2 Where business mobile phones and portable devices are not issued by Nursing Direct, staff including Agency Workers may be required to use a personal device in relation to their work.

4.3 Personal mobile phones and portable devices are the responsibility of staff including Agency Workers to ensure regular checks and maintenance of the devices are carried out to ensure they remain functional, secure and that the phone battery is charged sufficiently at all times.

4.4 Nursing Direct accepts no responsibility or liability for the loss, theft, or damage of personal mobile phones and portable devices. Staff including Agency Workers must ensure their phones are kept securely when not in use. It is strongly recommended that all devices are fitted with a protective case and screen protector. Staff including Agency Workers are also advised to obtain appropriate insurance cover for their mobile phone.

4.5 **MINIMUM SECURITY REQUIREMENTS**

All personal devices used for work purposes must have the following security features enabled:

- Password and/or biometric lock
- Automatic lock after a short period of inactivity
- Full device encryption

4.6 Failure to adhere to any part of this policy and procedure, either by omission or commission, is a disciplinary offence and may lead to dismissal.

4.7 All mobile phones/portable devices used as a work tool:

- Will be set with a secure password
- Will be updated regularly with the latest security patches and software updates
- Will only be used when driving if it is legal to do so. Bluetooth, hands free and the use of other technology that supports the safe use of mobile phones when driving must be used at all times
- Must be used safely and in line with the requirements of this policy
- Camera and voice recording facilities will only be used when consent is given

4.8 **APPROVED APPLICATIONS ONLY**

Only applications approved by Nursing Direct may be used to access, store or communicate work-related information. Unapproved communication apps (e.g. WhatsApp, Messenger, social media messaging) must not be used for work purposes unless explicitly authorised.

4.9 **DATA MINIMISATION ON PERSONAL DEVICES**

Where personal devices are authorised for work use, staff including Agency Workers must ensure that work-related information is held only temporarily and deleted immediately once transferred to the correct system. Personal devices must never permanently store sensitive or confidential Service User information.

Any personal mobile phones and portable devices must be used safely and in line with the requirements of Nursing Direct detailed in this policy.

5. PROCEDURE

5.1 **MOBILE PHONE CONDUCT**

Staff including Agency Workers will ensure that, when using a mobile phone for any work purposes, conversations are kept confidential. If discussing Service User matters, the conversation must be made out of the hearing range of anyone not authorised to have the information.

Staff including Agency Workers must not communicate over the phone in a manner which is not professional, or which is in any way harassing, intimidating or discriminatory towards others.

5.2 **CONFIDENTIALITY IN PUBLIC AND SHARED SPACES**

Staff including Agency Workers must avoid discussing confidential matters in public or shared spaces. Speakerphone use must be avoided unless in a private area where conversations cannot be overheard.

5.3 Staff including Agency Workers must check the signal reception on the phone and familiarise themselves with signal black spots. Staff will follow Lone Working procedures.

5.4 **TEXT MESSAGES**

Staff including Agency Workers may use their personal mobile phone to make calls or send text messages only where this is necessary for work purposes, such as coordinating visits, contacting the office/on-call team, or responding to service user-related queries in line with role requirements. Staff including Agency Workers must not use their personal phone to send confidential or sensitive information about a service user via SMS, WhatsApp, Messenger, or other messaging platforms, unless this is specifically authorised and an approved secure method is in place.

All communication must be professional, respectful, and proportionate, and must comply with data protection requirements and Nursing Direct confidentiality standards. Staff including Agency Workers must ensure that service user details are not visible to others (e.g., on lock screens/notifications) and should delete unnecessary messages as soon as practicable in line with record keeping expectations. Where a communication relates to care delivery, concerns, incidents, or safeguarding matters, it must be recorded appropriately (e.g., within the OneTouch App and/or through the relevant reporting process).

5.5 **USE OF APPLICATION FACILITIES**

Where required for the delivery of care, staff including Agency Workers must download and use approved work-related applications, such as the OneTouch App, on their personal mobile phone or portable device. These applications are used to support care delivery, including recording care notes and other relevant information relating to the service user.

Staff including Agency Workers must ensure that any work-related applications are used solely for work purposes and in accordance with Nursing Direct policies on confidentiality, data protection, and information governance. Devices used to access these applications must be secured with appropriate protections (e.g., PIN, password, or biometric lock) to safeguard service user information. Staff including Agency Workers must not share their login details or allow others to access work-related applications on their device.

5.6 **APP PERMISSIONS**

Staff including Agency Workers must not grant apps unnecessary access permissions such as camera, microphone, storage, or location unless required for work and approved by Nursing Direct.

5.7 **USE OF THE INTERNET / BROWSING THE INTERNET**

Staff including Agency Workers may use the internet on their personal mobile phone during working time only where this directly supports their duties, such as accessing the OneTouch App, obtaining essential work-related information to support safe care, or contacting Nursing Direct systems/services where required. Personal browsing and social media use must be kept to break times only and must never interfere with supervision of, engagement with, or the safety of service users.

5.8 **USE OF PUBLIC WI-FI**

Use of Public wi-fi should be regarded as a last alternative. There are two basic kinds of public Wi-Fi networks - secured and unsecured.

An unsecured network can be connected to within range and without any type of security feature like a password or login. Conversely, a secured network requires a user to agree to legal terms, register an account, or type in a password before connecting to the network. It may also require a fee or store purchase to gain access to the password or network.

Regardless of the connection type, **you should always use public Wi-Fi with caution.**

- **Do connect** to secured public networks whenever possible. In the event that you are unable to connect to a secured network, using an unsecured network would be permissible if the connection requires some sort of login or registration
- **Do not** access personal bank accounts or sensitive personal data on unsecured public networks. Even secured networks can be risky. Use your best judgment if you must access these accounts on public Wi-Fi
- **Do not** leave your laptop, tablet, or smartphone unattended in a public place. Even if you are working on a secure Wi-Fi network, that will not stop someone from taking your property or sneaking a peek at your device
- **Do not** shop online when using public Wi-Fi. Sure, shopping does not seem like it involves sensitive data, but making purchases online requires personal information that could include bank account and retailer login credentials. Shopping is not something you want to do on an unsecured Wi-Fi network
- **Do** turn off automatic connectivity. Most smartphones, laptops, and tablets have automatic connectivity settings, which allow you to seamlessly connect from one hotspot to the next. This is a convenient feature, but it can also connect your devices to networks you ordinarily would not use. Keep these settings turned off, especially when you are travelling to unfamiliar places
- **Do** monitor your Bluetooth connectivity. Bluetooth in the home is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can pose a huge risk to your cybersecurity. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked down when you leave your home, office, or similar secured area
- **Do** think about using a virtual private network (VPN) solution to ensure your privacy and anonymity are protected when you use public Wi-Fi. VPN services, like the new Norton Secure VPN, can encrypt all the data that you send and receive while using a public Wi-Fi hotspot, securing your information from other users of the same connection

5.9 **USE OF PERSONAL PORTABLE DEVICES**

Where staff including Agency Workers at Nursing Direct have been approved to use their own devices for work purposes, for example to support meetings via video, mobile messaging, and home working, where there is no practical alternative, reasonable steps must be taken to ensure that using their own device is safe.

Staff including Agency Workers at Nursing Direct must ensure that they set a strong password, use secure channels to communicate, e.g. tools/apps that use encryption, and ensure the device does not store personal/confidential Service User information, unless absolutely necessary, and that the appropriate security is in place.

Information must be safely transferred to the appropriate care record as soon as practical and the original deleted. In all video meetings UK GDPR / Data Protection Act laws and principles must be followed.

Where work emails are linked to personal devices these must be managed in line with UK GDPR / Data Protection requirements and information must not be shared inappropriately.

If personal portable devices are used to take photographs, as agreed by Nursing Direct, this must be conducted in line with the Computer, Email and Internet Usage Policy and Procedure at Nursing Direct.

When a personal portable device is no longer used for work purposes all Nursing Direct information must be removed from the device. A weekly purge is recommended as best practice of all information that is no longer used or required. Nursing Direct is not responsible for maintaining or replacing privately owned devices.

5.10 TEMPORARY STORAGE ONLY ON PERSONAL DEVICES

All work-related information accessed via personal devices must be held temporarily and transferred to the relevant system as soon as practical. The data must then be deleted from the personal device.

5.11 WEEKLY PURGE REQUIREMENT

Staff including Agency Workers must conduct a weekly review and deletion of all temporary work-related information held on personal devices, ensuring no residual Nursing Direct data remains.

5.12 REPORTING TECHNICAL OR SECURITY ISSUES

Any security warnings, loss of functionality, or suspected malicious activity must be reported immediately to Nursing Direct.

5.13 IN THE EVENT OF LOSS AND/OR DAMAGE

If any equipment or device used for work purposes (including a personal mobile phone used to access the OneTouch App or to support care delivery) is lost, stolen, or damaged, this must be reported to Nursing Direct immediately and as soon as the loss/damage is identified.

Where the device may contain, display, or provide access to service user information (including via apps, emails, messages, photos, or saved documents), the incident will be assessed and may require escalation and reporting in line with data breach/UK GDPR requirements and Nursing Direct's information governance procedures.

Staff including Agency Workers must cooperate with any actions required to protect information (e.g., changing passwords, disabling access, remote wipe where available) and must not delay reporting.

Immediate Security Actions When Device Lost/Stolen

When reporting a lost or stolen device, staff including Agency Workers must:

- Notify Nursing Direct immediately
- Confirm last known location
- Provide details of any Service User information accessed
- Cooperate with remote lock or remote wipe actions

Complete an incident form within 24 hours

6. DEFINITIONS

6.1 MOBILE APPLICATIONS (APPS)

A mobile app is a software application developed specifically for use on small, wireless computing devices, such as smartphones and tablets, rather than desktop or laptop computers


6.2 INTERNET BROWSER

An internet browser, also known as a web browser or simply a browser, is a software program that you use to access the Internet and view web pages on your mobile phone or computer

OUTSTANDING PRACTICE

To be "outstanding" in this policy area you could provide evidence that:

- Nursing Direct carries out confidentiality and data protection monitoring and spot checks
- Risk assessments are in place, and Nursing Direct ensures that these are regularly checked and updated, and that staff including Agency Workers understand their obligations under the Health and Safety at Work Act
- Staff including Agency Workers report effective communication when accessing colleagues, either when on call or outside of the service

COMPLETED DATE:	05.03.2026
SIGN OFF DATE:	05.03.2026
REVIEW DATE:	05.03.2027
SIGNED:	 Marc Stiff – Group Managing Director