Western Health and Social Care Trust

Mobile Telephone and Device Policy

March 2020

Version 3.8

Policy Title	TRUST MOBILE TELEPHONE AND DEVICE POLICY
Policy Reference Number	Corp20/001
Implementation Date	March 2020
Review Date	March 2022
Responsible Officer	FERGAL DUREY, AD for ICT and Telecommunications

Table of Contents

1 Background and Purpose

Mobile telephones are a major communication tool for both the private individual and business user. This technology is highly dependent on network coverage.

No network provider will guarantee 100% coverage or service!

The Department of Health states that use of mobile phones within NHS sites should be allowed as long as their use does not affect:

- The safety of service users (Patients , Clients)
- Service users privacy and dignity
- The operation of medical equipment

The Western Health and Social Care Trust (WHSCT) has a separate policy for service users, visitors and staff in **Mental Health Wards** and should be read in conjunction with this policy.

For WHSCT staff, mobile telephones and devices represent a significant communication, business and information tool and thereby staff need to be aware of their personal responsibilities with regards to their use and the potential consequences resulting from misuse. These devices often provide additional functionality i.e. Information & Communication Technology (ICT) including the capability to access the internet and use camera and video recording functions and music players.

The WHSCT recognises that staff, carers, visitors and service users should be able to use mobile telephones and devices, where it is appropriate to do so and subject to medical and privacy considerations.

This policy has been developed to ensure proper use of mobile telephones and devices by making Trust staff, service users and visitors aware of the statutory legal obligation and the organisation's definition on acceptable and unacceptable use.

This policy has also been developed to make service users and visitors aware of the areas where the use of mobile phones and devices are restricted or limited.

The measures outlined in this policy will not be effective without the cooperation of all WHSCT staff. These include full-time, part-time, 3rd party consultants contracted by the Trust to work on specific projects, agency and temporary employees including students and volunteers. The cooperation of all such staff, and acceptance of this policy, is therefore a prerequisite to approval for mobile telephone and device use.

2 Scope

In the context of this policy the term mobile telephone also refers to smart telephones.

This policy applies to all those working in the WHSCT, in whatever capacity, covers all Trust and *personally* owned mobile telephones and devices as part of their duties. This policy covers all standard functionality supplied with a mobile phone including, but not limited to, making and receiving calls, sending and receiving of text messages, taking and storing pictures, downloading apps etc.

Any member of Trust staff seeking to acquire a Trust mobile telephone should refer to the procedure in Appendix 2.

This policy also applies to service users and visitors to the Trust whilst on Trust premises.

3 Medical Photography

There are stringent medical legal and professional standards to be met and in order to do so it is anticipated that all medical photography should be undertaken by trained medical photographers. The Trust however accepts that there are specific occasions where trained operators, who are not medical photographers, may be required to document a clinical episode, on Trust owned equipment. The use of personal recording devices, cameras smart phones or any other recording device is prohibited unless a Trust approved encrypted supplication is used.

Out of hours cameras, Trust owned, are available in Theatres, Emergency Departments and the Labour Wards.
Other Trust owned cameras are available to Tissue Viability nurses and Community Podiatrists.

The reader is referred to the Western Trust's *Data Protection and Confidentiality Policy* and Section 2.3 in particular.

For any queries contact the Medical Photography department in Altnagelvin Hospital.

4 Code of Conduct

4.1 Guidelines for Everyone

a) Where a service user, a member of the public, visitor or a member of staff brings a privately owned mobile device onto a Trust site they do so at their own risk. The Trust will not be held responsible for any device that is lost, stolen, or damaged.

b) Everyone must be mindful of moderation of tone, volume and language and may be informed if behaviour is deemed disruptive. Telephone ringing and subsequent conversations may disrupt important service user healthcare professional activities or may disturb and/or alarm service users who are resting

c) The Trust **prohibits** the use of *USB ports/sockets on any Trust equipment* for the charging of mobile devices and phones.

d) must switch phones to silent in restricted areas (refer to Appendix 1 for guidelines for areas of use)

e) must be mindful of the risk of spreading infection when using mobile devices or phones

f) users who wish to make a phone call after 10pm and before 7am must find a local permitted area e.g. corridor

g) the use of camera phones, or any camera, may compromise service user confidentiality. Service user's confidentiality, dignity and privacy **must be** respected at all times.
If a service user or member of staff is identifiable in the image then their consent **should be** sought in advance.

h) Service users, relatives and other visitors are **not** permitted to photograph or video Trust staff without their consent.

i) Service users, relatives and other visitors are **not** permitted to photograph or video their records. Copies of medical care notes can be formally requested via a "Subject Access Request" (SAR) application.

j) Everyone must be mindful that any part of a covert or overt recording of a service users consultation, which is private and confidential, that is disclosed or published without prior consent with the other recorded parties may be committing a **criminal offence**, e.g. breach of the Data Protection Act 2018

k) The misuse of a recording may result in a **breach of legislation** and possible legal action, e.g. for defamation.

l) For other devices, i.e. Laptop Computers/Tablets/Gaming Devices, enabled with wireless network capabilities must also adhere to this code of conduct as well as Trust ICT policies regarding the Internet.

4.2 Service Users

a) Service users may record their personal consultation or treatment for their **personal** use. It should be noted that it is *common courtesy* to ask for consent and that any **misuse** of the recording lies with the service user.

b) Any recording must **not interfere** with the consultation, treatment or care being administered otherwise the service user will be asked to stop recording.

c) Where a service user has made a recording, a note should be made in the service user's medical file by Trust staff.

d) Trust staff can **refuse** to participate in any recordings where there is a concern of an intention to use the recording for malicious purposes.

4.3 Areas of Use

Refer to Appendix 1 for a guide to areas where Mobile Phones and devices can and cannot be used.

Service users or visitors who fail to adhere to the policy will be asked to leave the "prohibited use" area. Security may be called if they become abusive or aggressive towards staff enforcing this policy, in line with the *Trust's Zero Tolerance and Security Policy*. *It should be noted the Trust does not accept the display of violence or aggression towards NHS staff whilst undertaking their work.*

4.4 Western Health and Social Care Staff

4.4.1 Use of a Mobile Phone/Device whilst driving

The Western Health and Social Care Trust **do not condone** the use of mobile telephones or devices whilst driving.

For further details the reader is referred to the "Road Vehicles (Construction and Use) Regulations 1986, Regulation 104"

Whilst it is not illegal to use a hands-free device whilst driving, depending on the circumstances, a driver could be charged with failing to have proper control of his or her vehicle.

The WHSCT will **not** be responsible for payment of any fines incurred under this Regulation.

4.4.2 Guidelines

Staff personal mobile phones or devices are their own responsibility when on Trust property.

Staff seeking to obtain a Trust mobile telephone should refer to the procedure in Appendix 2.

Staff who lose, or fail to return on leaving employment, a Trust owned mobile phone or device, will have the devices cost charged back to their Directorate.

4.4.2.1 Information Governance

Information Governance is seen as a key risk when dealing with Trust owned and personal mobile telephones or devices, therefore in conjunction with this policy, Trust staff are advised to refer to the Western Trust's *Data Protection and Confidentiality (DP&C) Policy.* The DP&C policy provides more detail on staff responsibilities, the handling of personal information, GDPR principles, photographic consent and compliance.

4.4.2.2 Service user recording a personal consultation or treatment

a) Service users should be discouraged from making any recordings but **can** record a personal medical consultation or treatment; however it would be a *common courtesy* for the Service user to ask for consent in advance. Service users can be advised that they are entitled to see their notes, if they so wish, via a "Subject Access Request" (SAR) application.

b) Where a service user intends to make a recording; the service user needs to be made aware of the private and confidential nature of the recording and **their responsibility** to keep it safe and secure. The service user should be made aware of the potential legalities if the recording is misused e.g. breach of Data Protection Act 2018, defamation, etc.

c) Trust staff can **refuse** to participate in any recordings where there is a concern of an intention to use the recording for malicious purposes.

d) Any recordings must **not interfere** with the consultation, treatment or care being administered otherwise the service user should be asked to stop recording.

e) When a service user does make a recording of their consultation or treatment, Trust staff should place a **note** in the service user health record. Trust staff need to inform the service user that this note states that the service user recorded the consultation or treatment.

4.4.2.3 Service users or visitors recording

a) Service users and visitors should be discouraged from making any photographs or videos; however it would be a *common courtesy* for them to ask for consent in advance.

b) Where a service user or visitor intends to take a photograph or video; the individual(s) needs to be made aware that **prior consent** is required from those Trust Staff and/or non-family members who may appear in the image(s) as well as the potential legalities if the recording is misused e.g. failure to gain consent is likely to breach the **Data Protection Act 2018**.

c) Where there is a concern of an intention to use a recording for malicious purposes staff should advise their manager.

4.4.2.4 Miscellaneous

Staff who are in possession of a Trust Mobile Phone shall accept full responsibility for the security of the device. Users of assigned Trust mobile phones and devices **must** make all reasonable efforts to secure the devices and protect against damage. E.g. do **not** leave Trust devices in parked vehicles.

a) Staff are **advised** to place mobile phones on silent, or vibrate, during meetings and during service user consultations.

b) Staff are reminded to ensure confidentiality and security is upheld when using Trust mobile telephones and devices in HSC and non-HSC locations. E.g. staff are advised **not** to discuss service users in public areas

c) Only Trust e-mail accounts can be configured on the Trust mobile telephones and devices

d) Service user Identifiable data must **not** be sent through the Short Message Service (SMS) on **any** mobile device

e) **No** attempt should be made to “unlock” a Trust owned mobile phone or device

f) Service user details and/or numbers must **not** be stored in **any** mobile telephone

g) Only Trust approved applications (apps) can be installed onto Trust mobile phones and devices.

h) Leaving Bluetooth enabled and in discoverable mode can enable an attacker to connect to the device and access information. Due to this security risk, it is **advised** that the Bluetooth facility on mobile phones **should be** turned *off/hidden* when not in use.

i) **Exceptionally** the use of audio, photographs or video may be necessary as part of a person’s work, e.g. to record the specific position of something for Health and Safety purposes and as part of incident follow up of investigation.

j) These guidelines **must be** read in conjunction with the WHSCT E-mail, Internet and Social Media policy guidelines.

k) Any data, texts or images recorded by mobile telephones or devices are subject to General Data Protection Regulation (GDPR) and Freedom of Information (FOI) Act 2000

l) Staff **must** be mindful of moderation of tone, volume and language when using mobile phones on Trust premises

m) Unless performed on an **"approved"** application from ICT, no data/information relating to any service user should be recorded, stored or sent using a mobile device. (E.g. photographs / documents etc)

n) Under **no** circumstances should a Trust mobile phone number be transferred to a personal mobile phone.

o) Charging of mobile phones and devices is only allowed when using an **official** (not generic) charger that has a valid PAT safety test certificate. Only spare power sockets can be used with an understanding that other devices will take priority where limited sockets are available. Mobile phone chargers will also have to be unplugged when not in use.

p) **Using a handheld mobile phone whilst driving is illegal**.

q) When staff are visiting service users in their own home, phones should be placed on silent and phone calls not accepted during this time unless urgent

r) Staff are **not** permitted to use a service user's mobile device without the service user's consent.

s) Staff are discouraged from using their personal mobile telephones for any Trust business unless a Trust approved encrypted application is used. Staff should **be aware** that Trust mobile phones have a security infrastructure supporting them and as a result are more secure than personal mobile phones.

The reader is referred to the Western Trust's *Data Protection and Confidentiality Policy* and Section 2.3 in particular.

t) All Staff are empowered to challenge the misuse of mobile devices on site

Staff who fail to comply with the policy will be reported to their line manager and persistent breaches of the policy will be dealt with under the Trust's disciplinary procedure.

To protect against unauthorised use, all Trust mobile telephone users **must** ensure that the PIN code / Password is configured.

All ‘smart’ phones issued by the Trust, with applications containing Trust data, will be managed by an approved Mobile Device Management encryption solution. This ensures that any data synchronised to the device is stored in an encrypted area of the device. If the device is lost or stolen the Trust shall use remote erase technology to delete any data stored on the phone and then disable it.

4.4.3 Usage

a) The use of personal mobiles in work is at line managers’ discretion, but any usage must not impact on the delivery of service.

b) Staff are reminded that they are **not** to store any client or service user identifiable data on their Personal Mobile phones or devices unless a Trust approved encrypted application is used.

   The reader is referred to the Western Trust’s *Data Protection and Confidentiality Policy*.

c) Personal Mobiles should be kept on silent, or kept with other personal items e.g. handbag, backpack etc. The **only exemption** being when a staff member needs their phone for Trust business (e.g. consultant on call).

d) The Trust recommends that staff switch off their Trust mobile telephone or activate voice mail facility prior to driving and pick up calls later when their journey has ended.

e) Trust staff are **not** to phone colleagues while they are known to be driving. Any driver, who does receive a telephone call, whilst driving, should **not** answer the call but let the call go to voicemail.

f) The user must **not** lend their Trust mobile telephone to any person **not** employed by the Trust.

g) In the case where the Trust mobile telephone is used by a team, the appropriate line manager **must** take overall responsibility for security and usage.

h) Users are **not to install or uninstall software** (apps) on Trust owned mobile phones or devices. Only authorised ICT staff can install/uninstall software.

i) Trust mobile telephones and devices that are in need of repair **must** be returned to the ICT Department. These will be returned to the supplier for repair or replacement. Manufacturer warranties do not normally cover damage caused by misuse or neglect and the cost of repairs will be borne by the assigned user.

j) **Any** loss or theft of a Trust mobile telephone or device **must** be reported immediately to their line manager and the Trust Telecoms Manager, in order to stop the telephone from being used. A DATIX incident needs to be completed by the user.

k) **Any** loss of a Trust mobile may incur a charge to the associated Directorate

4.4.4 Mobile Telephone user leaving the Trust

a) When an employee leaves the Trust, their Trust mobile telephone, SIM card and any sundry kit remains Trust property and it is the **Line Manager's responsibility** to ensure that the items are returned by the employee. It is also the **Line Manager's responsibility** to make arrangements for the returning of this kit to the ICT Department, along with all relevant details e.g. user, mobile number etc, so that the correct Disposals procedure can be adhered to.

b) Should a user fail to return their Trust mobile telephone to the Trust they will be held responsible for any calls, line rentals or loss of the mobile telephone.

c) Users are again reminded of their responsibilities regarding GDPR, FOI etc.

4.4.5 Long Term Absence

- Where Trust staff are on maternity leave or other long term absence, including secondment, they should ensure that the Trust mobile, or any Trust owned device, is returned to their line manager through the most appropriate means.

4.4.6 Transferring of Trust mobiles or devices within Directorates / Departments

- Should an employee, or manager, have cause to transfer a Trust mobile or device to another member of staff within the Directorate/Department they should log the details of the transfer on the ICT Helpdesk. Redistribution of "smart" phones, containing personal data, is subject to the GDPR and Computer Misuse acts. The following details should be provided;

    - Mobile number
    - Current user
    - New user
    - Department
    - Directorate
    - Cost centre

5 Disposal of Trust owned Mobile Phones

a) It is ***the user's responsibility*** to transfer any contact details on a Trust mobile phone to another device before surrendering for disposal.

Users are reminded of their responsibilities regarding GDPR, FOI etc.

b) The ICT department will dispose of Trust mobile phones in line with the ICT Disposals Policy

c) Trust Mobile phone SIMS and memory cards will be physically destroyed and will not be recoverable.

d) The ICT department is not liable for the retrieval of data recorded on any mobile phone, SIM and memory cards.

6 Incident Reporting

Staff should report any actual or suspected breaches of confidentiality or data security with regard to Mobile phones or devices via the Trust's incident reporting procedure.

Staff should report any loss or theft of a Trust owned mobile phone or device via the Trust's incident reporting procedure. A DATIX incident needs to be completed.

7 Countermeasures

- **Security**
  The Trust reserves the right to perform a 'remote wipe' to all Trust mobile telephones configured for access to Trust systems to ensure protection of the Trust's data. This function, once actioned, will remove all data including contacts, messages, photographs etc from the device.

- **Monitoring**
  i) The Trust reserves the right to monitor the Trust mobile telephone usage and may, with appropriate approval, gain access to the mobile telephone in the absence of a member of staff.
  ii) Suspected cases of abuse on the system or breaches in policy will be rigorously investigated by ICT, and where necessary, in conjunction with HR staff.

- **Removal**
  i) Mobile telephones may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected abuse or misuse
  ii) Mobile telephone accounts will be terminated (and data on the device archived) for staff who leave the organisation.

8 Additional Resources

This policy should be read in conjunction with other policies relating to effective and appropriate use of ICT services, including

- WHSCT Internet Policy
- WHSCT Social Media Policy
- WHSCT Data Protection and Confidentiality Policy
- WHSCT Policy for Use of Mobile Devices / Phones in Mental Health Wards
- WHSCT Zero Tolerance and Security Policy
- *Freedom Of Information & E-mails Guidance (issued by WHSCT Communications Department)*
- DHSSPS – Code of Practice on Protecting the Confidentiality of Service User Information
- Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
- Information Commissioner – Data sharing code of practice (www.ico.gov.uk)
- Regulation of Investigatory Powers Act 2000
- Department of Transport (2007)
- Road Vehicles (Construction and Use) Regulations 1986, Regulation 104
- The Royal Society for the Prevention of Accidents (2007) Driving for Work: Mobile Telephones
- Information Governance Alliance – The use of Mobile Devices in Hospitals
- NHS Guide – Patients recording NHS staff in health and social care settings
- WHSCT - Waste Manual:- Section 5.1 Waste Electrical and Electronic Equipment (WEEE)
- Computer Misuse Act 1990
- Information Governance Alliance (IGA) – The use of Mobile Devices in Hospitals (e.g. Phones, Tablets and Cameras)
- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- WHSCT - Good Practices and Email Etiquette
- Dept of Health - Co-operating to Safeguard Children/Young People in NI
- Dept of Health – Code of Conduct
- WHSCT Management of User Accounts and Password Policy.
- WHSCT Server, Desktop and Portable Security Policy
- WHSCT Malicious Software Policy
- WHSCT Disposals Policy (incl redistribution of ICT equipment)
- BSO ICT policies

9 Training

The Trust is committed to staff development and seeks to consistently improve development standards and opportunities for staff in line with organisational objectives, policies and procedures.

9.1 General ICT Training

Should you or your staff require support in the effective use of ICT please contact the ICT Training Team via the ICT Service Desk.

9.2 E-Learning

9.2.1 Mandatory Training

Mandatory Training, either set out by legislation or Trust, is compulsory for all staff and is intended to ensure that Trust staff are aware of their responsibilities to comply with set standards.

A number of Mandatory courses are available through E-Learning such as WHSCT_Equality, Good Relations and Human Rights training. The aforementioned training can be accessed via the following link: http://www.hsclearning.com/

9.2.2 Cyber Security (as defined in Section 2 of this document)

The Western Health and Social Care Trust have invested in a software solution from Metacompliance Ltd to help ensure that the WHSCT ICT security expectations are understood by Trust staff. This is an E-Learning platform which enables the Trust to push out awareness content to Trust staff. This provides education regarding Cyber Security topics and the importance of Good Practice and Trust policies and thereby protects the organisation from potential attack.

This tool is designed to be intuitive and flexible so that Trust staff can easily register and undertake training at a time and place that suits them.

Note: Lessons learnt from this training, e.g. Phishing emails, can also be applied to the individual's home environment.

10 Equality & Human Right's Statement

The Western Health & Social Care Trust's Equality and Human Right's statutory obligations have been considered during the development of this policy.

11 Further Information

For further information in relation to this policy please refer to:-

The ICT User Forum on the ICT service desk portal available on the Trust intranet link below.

(http://wta-eservicedesk/portal/)

Appendices

Appendix 1 - Hospital areas of use for Visitors, Service Users and Trust Staff

The Western Trust adopts the guidelines provided by the Information Governance Alliance regarding the use of Mobile Devices for areas of use.

"THE USE OF MOBILE DEVICES SHOULD BE KEPT TO A MINIMUM AND MUST ONLY BE USED WHERE ALLOWED. USERS OF MOBILE DEVICES MUST BE CONSIDERATE OF PATIENT PRIVACY, DIGNITY AND NEED FOR QUIET"

Area	Designation	Staff	Patients	Visitors
Intensive Care / High Dependency Units Operating Theatres and Recovery Areas Neonatal Units Emergency/ Resuscitation Areas Renal Dialysis Units Delivery Rooms Mental Health facilities	Prohibited	The use of personal mobiles is at line managers' discretion, but any usage must not impact on the service. Staff with carer responsibilities should agree a landline contact with their line manager	**Not allowed** The Nurse in Charge can agree exceptional patient use for those with specific communication or carer needs or for those confined to bed areas. Care should be taken to avoid creating a nuisance or disturbance to other patients / clients or staff.	**Not allowed** Visitors should leave the area. Calls must only be made from a permitted area or outside the building. The Nurse in Charge can agree exceptional use.
Other clinical areas (not in prohibited list) that the Trust has designated as restricted due to risks outweighing the benefits to patients and visitors.	Restricted	The use of personal mobiles is at line managers' discretion, but any usage must not impact on the service. Staff with carer responsibilities should agree a landline contact with their line manager	**Not allowed** The Nurse in charge can agree exceptional patient use as above but this should avoid proximity electronic Medical Device e.g. on Maternity Units pictures can be taken of new born babies if this is the ONLY method of taking the picture.	**Not allowed** Visitors should leave the area. Calls must only be made from a permitted area or outside the building The Nurse in Charge can agree exceptional use.
Other areas e.g. waiting areas	Permitted	The use of personal mobiles is at line managers' discretion, but any usage must not impact on the service. Staff with carer responsibilities should agree a landline contact with their line manager	**Allowed** but please have regard to others and try to keep a distance from electronic medical devices. Phones should not be used between 22:00 and 07:00. If using video chat the camera must be facing you and you need to be aware that you may pick up other people's conversations and other people may hear both sides of your conversation. Please Respect staff and service user privacy and dignity when updating your status on any social media sites / apps.	

VIDEO / PHOTOGRAPHS OF PATIENTS MUST NOT BE TAKEN ON PHONES BY PATIENTS OR VISITORS WITHOUT CLINICIALLY RESPONSIBLE STAFF AGREEMENT. KEEPING A RECORD OF YOUR OWN CARE IS PERMITTED BUT PLEASE INFORM STAFF IN ADVANCE AND HAVE REGARD TO THE PRIVACY AND DIGNITY OF OTHERS.

Appendix 2 - Procedure for Obtaining a Trust Mobile Telephone

Mobile telephones are provided to staff to ensure operational effectiveness and to aid communications.

All staff should be aware that Trust mobile telephones and devices must be ordered via the ICT department.

Prior to ordering new mobile devices Directors should ensure that all mobile devices currently operational within their respective Directorates are being appropriately utilised. Where it is decided that a mobile device can be re-allocated to another member of staff, within respective Directorates, the name of the new staff member should be logged on the ICT helpdesk as the new user.

Requestors for new mobiles must meet one of the criteria below and have approval from their Director, before a new mobile can be used. Respective Directors will have to supply a cost centre to allow for recharging.

The decision to approve the assignment of a WHSCT mobile phone device to an employee must only be made after careful consideration and examination of the employee's duties. A WHSCT mobile phone device must only be issued to employees who meet at least one of the following criteria:

a) The employee spends significant periods of time out of the office or normal place of work undertaking their duties;
b) The employee is on an official on-call rota;
c) The employee has been identified as a key member of staff and needs to be contactable at any time;
d) The employee's duties are such that the mobile phone device is needed for health and safety reasons;

The supplier, service provider, consultancy, equipment manufacture will be that determined by the Telecommunications Manager and where appropriate in line with current Framework Agreements. This is so to ensure, standardisation is achieved, Trust Policies and Financial standing orders and procurement processes are followed and are adhered to, equipment is system compatible, and to reduce the cost of ownership where possible.

The ICT department has in place a process for service users to request new /replacement or upgrading of equipment or services, via the ICT Mobile Devices Order Form which is available on the Trust intranet. This process will include the Telecoms Manager assessing the overall suitability of a request, ensuring that requested equipment will be fit for purpose, is the correct solution, is cost effective, future proofed and in line with the Trust's development programs.

Staff and Managers should note :

1. ***Redistribution of <u>any</u> ICT equipment, containing personal data, is subject to the General Data Protection Regulation (GDPR) and Computer misuse acts.***
2. ***It is the responsibility of departmental managers to complete an ICT equipment movement form for any equipment that is to be reassigned or returned to ICT department.***
3. ***Managers are advised to consult with the ICT Operations Manager if they have any doubts or queries regarding the redistribution of ICT equipment.***
4. ***Managers are advised to consult with the ICT Telephony team regarding the redistribution of Trust mobile phones.***
5. ***Any Trust mobile phone which has been returned to the ICT department may be redistributed by the ICT Telephony team depending on the needs of the service.***
6. ***Personal data should not be stored on a Trust mobile device. The Trust will not claim any responsibility for the loss of personal data stored on a Trust mobile device and the Telecoms team will not restore any personal information or data, including photographs, sound/video recordings, SMS messages, Memo's or down loaded applications, ring tones etc..***
7. ***Subscription by members of staff to text messaging services (e.g. sports results, news updates etc.) are prohibited from Trust mobile devices. Members of staff will be liable for any such subscriptions or any other unauthorised personal use.***
8. ***SIM cards must not be exchanged between mobile phones without the knowledge and approval of the Telecoms team. Use of dual SIMs requires approval from the Telecoms Manager.***
9. ***Owners of Trust mobile phones are responsible for reimbursing the Trust for any personal calls made using the mobile phone.***
10. ***Owners of Trust mobile phones are responsible for any call – business or private - made using the phone. Therefore owners of Trust mobile phones must not allow any other person to make use of their phone.***

Western Health and Social Care Trust	**Information Sheet:- The use of Mobile Phones and Devices on Trust Premises by Patients, Clients and Visitors**

Do's

- Place mobile phone on **silent** in restricted areas e.g. Intensive Care, High Dependency Unit, Neo-Natal, Mental Health facilities. Refer to next sheet
- **Respect** the confidentiality, dignity and privacy of patients and others at all times
- Be **mindful** of moderation of tone, volume and language. A telephone ringing and conversations may disrupt healthcare activities or disturb or alarm resting patient / clients
- Be mindful of the risk of spreading **infection** when using mobile devices or phones
- When using a mobile phone or device **after 10pm or before 7am**, use a local permitted area e.g. corridor

Don'ts

- Become a **victim** of theft! Take care of your personal device and property.
  The Western Trust will not be held responsible for any device that is lost, stolen, or damaged.
- Use a mobile phone within 1metre (3 feet) of **active** infusion pumps and monitors
- Use ***USB ports/sockets*** on any Trust equipment for charging of <u>any</u> equipment including mobile phones and devices
- Use power sockets that have Trust equipment **already** plugged into them.
- Compromise patient, client, visitors or staff confidentiality by using **any camera**, including mobile phones. Prior permission is required from Clinically Responsible Staff

  Maternity units may permit photographs to be taken with a mobile phone or device, for example, parents with their new-born baby **as long as** no staff or other service users are in the photograph.

For further information please refer to the Western Trust's Mobile Telephone and Device Policy

Hospital areas of use for Visitors, Patients and Clients

The Western Trust adopts the guidelines provided by the Information Governance Alliance regarding the use of Mobile Devices for areas of use.

"USERS OF MOBILE DEVICES MUST BE CONSIDERATE OF PATIENT PRIVACY, DIGNITY AND NEED FOR QUIET"

Area	Designation	Patients / Clients	Visitors
Intensive Care / High Dependency Units Operating Theatres and Recovery Areas Neonatal Units Emergency/ Resuscitation Areas Renal Dialysis Units Delivery Rooms Mental Health facilities	Prohibited	**Not allowed** The Nurse in Charge can agree exceptional patient use for those with specific communication or carer needs or for those confined to bed areas. Care should be taken to avoid creating a nuisance or disturbance to other patients / clients or staff.	**Not allowed** Visitors should leave the area. Calls must only be made from a permitted area or outside the building. The Nurse in Charge can agree exceptional use.
Other clinical areas (not in prohibited list) that the Trust has designated as restricted due to risks outweighing the benefits to patients and visitors.	Restricted	**Not allowed** The Nurse in charge can agree exceptional patient use as above but this should avoid proximity electronic Medical Device e.g. on Maternity Units pictures can be taken of new born babies if this is the **ONLY** method of taking the picture.	**Not allowed** Visitors should leave the area. Calls must only be made from a permitted area or outside the building. The Nurse in Charge can agree exceptional use.
Other areas e.g. Wards, waiting areas	Permitted	**Allowed** but please have regard to others and try to keep a distance from electronic medical devices. Phones **should not be used** between **22:00** and **07:00**. If using video chat the camera must be facing you and you need to be aware that you may pick up other people's conversations and other people may hear both sides of your conversation. Please Respect staff and service user privacy and dignity when updating your status on any social media sites / apps.	

VIDEO / PHOTOGRAPHS OF PATIENTS MUST NOT BE TAKEN ON PHONES BY PATIENTS OR VISITORS WITHOUT CLINICIALLY RESPONSIBLE STAFF AGREEMENT. KEEPING A RECORD OF YOUR OWN CARE IS PERMITTED BUT PLEASE INFORM STAFF IN ADVANCE AND HAVE REGARD TO THE PRIVACY AND DIGNITY OF OTHERS

Staff have the right to refuse patients/clients, their representatives and other visitors the use of photographic and recording equipment

Staff have the right to refuse patients/clients, their representatives and other visitors the use of photographic and recording equipment