Telecoms Policy

Owner: Simon Carey

Version: 5.5.0

Hertfordshire, Bedfordshire, and Luton ICT Shared Services is hosted by NHS Hertfordshire and West Essex Integrated Care Board

Copyright

Document Control

Document Owner	Simon Carey	**Approved by**	HBL ICT SMT
Document Author(s)	Victoria Robinson, Keith Fairbrother, Alex McLaren, Usman Khan, Nick Downer, Gisella Harris, Simon Hassall	**Date of Approval**	14th November 2023
Version	5.5.0	**Date for Review**	12 months

Version Control

Version	Status	Commentary	Date	Author
0.A	Draft	Initial Draft (replacing Mobile Phone Policy)	10/2014	K Fairbrother/ V Robinson
0.B	Draft	Additions and Amendments	11/2014	V R
1.0	Live	HBL ICT SMT Approval	01/2015	HBL ICT SMT
1.1	Live	Addition of Section 4.16	08/2015	P Parker
1.2	Live	HBL ICT SMT Approval. Format change	10/2015	HBL ICT SMT
1.3	Draft	Following TR updates, and into new format. For full review in 17/18	12/2016	A McLaren
2.0	Live	Ownership to A McLaren	3/2017	A McLaren
2.01	Draft	In review for GDPR	11/2017	A McLaren
3.0.0	Live	Authorised by Phil Turnock	29/11/2017	A McLaren
3.0.1	Draft	Annual Review Addition to reference section (NHS Digital Telecoms Example Policy), remove image of asset tag from terms and acronyms Insert section Telephone Security, Fax Security, Handheld Radio Security (from NHS Digital template)	Nov 2018	A McLaren; U Khan

Version	Status	Commentary	Date	Author
		Insert Terminology section (from NHS Digital template) Updates 2.0 Introduction – clarification including Line Managers responsibility 3.0 clarification of eligibility; 3.2 links to information; 3.9 clarification, 3.14 amend to social networking; 3.17 transfer costs highlighted		
4.0.0	Live	Approved by SMT	26/11/2018	A McLaren
4.1.0	Live	Update to 3.8 to reflect Data Protection	6/12/2018	A McLaren
4.1.1	Draft	Annual review, no changes confirmed	11/11/2019	U Khan
5.0.0	Live	Approved by SMT	14/11/2019	A McLaren
5.0.1	Draft	Annual review – no changes confirmed	Aug 2020	A McLaren
5.1.0	Live	Approved by SMT	1/9/2020	A McLaren
5.1.1	Draft	Update to Implementation plan replacing IG Toolkit with DSPT	Oct 2020	A McLaren
5.2.0	Live	Approved by SMT	3/11/2020	A McLaren
5.2.1	Draft	Annual update –changes to dept and roles, document ownership	Nov 2021	A McLaren
5.3.0	Live	Authorized by SMT	16/11/2021	A McLaren
5.3.1	Draft	Annual review Document template/format updated CCG references updated to ICB HBL ICT Department names updated Internal reference documentation – Names of policies updated External legislation – Reference to EU legislation removed. GDPR changed to UKGDPR Network technology updated to include 5G Accessibility Considerations section added to policy following EQIA review. Mobile Device request form removed from document and replaced with link to ServiceNow.	Oct 2022	S Hassall
5.4.0	Live	Authorised by SMT	1/12/2022	S Hassall
5.4.1	Draft	Annual review InTune references, as a Mobile Device Management platform, included in document. References to GDPR updated to UK GDPR.	September 2023	N Downer, G Harris, S Hassall

Version	Status	Commentary	Date	Author
5.5.0	Live	Authorised by HBL ICT SMT	14/11/2023	S Hassall

Terms and Acronyms

Term	Definition
Apple ID	A unique corporate/user ID used in creating an ITunes account for use with an Apple iOS device.
CSAR Form	The form a customer is required to submit in order to obtain a user account on the Organisation's Nebula IT network. By signing the form the customer is agreeing to abide by Organisation policies surrounding acceptable user of Computers, the Network and E-Mail and Internet. These policies and principles extend to the user's usage of Mobile Phone and Data Devices.
Data Protection Act and UK GDPR	These Acts define the laws which apply to the UK for the storage, processing and transportation of data relating to identifiable living people. You are governed by it when you 'process personal data'. This is a strict legal definition but, broadly speaking, you are very likely to be processing personal data if you deal with any patient records, any staff records or have any dealings with the general public. As an NHS employee you are required to comply with the requirements of this act.
GDPR / UK GDPR	General Data Protection Regulation. An EU wide regulation from 25 May 2018. This later became UK GDPR after the UK's exit from the European Union.
Location Services	Allows remote location-tracking mobile devices as well as comprehensive security and app capabilities. A mobile IT administrator can manage the lifecycle of the device and its apps, from registration to retirement, and quickly get mobile operations under control. The other features include the ability for the administrator to manage devices from a central web-based console, configure devices, set policies for encryption and lockdown, enforce restrictions and complex passwords, remotely lock and wipe devices, and allow end-user self-service for their devices. Additionally, the platform supports management of app inventory, the ability to create an enterprise app storefront, and provides protection from rogue apps.
Mobile Data Device	There is no one definition for this term as it can encompass a broad range of devices from Calculators to Digital Camcorders. For the purpose of this policy we are referring to an Organisation issued device which can send or receive data using either Wireless LAN or Mobile Phone Networks. Typically these devices include Mobile Phones, Smart Phones and Mobile Data connections via SIM only, a mobile data stick or a tablet device.
Mobile Data Stick/Dongle	This small USB device contains a mobile modem and allows the connected computer to send and receive data using the Mobile Network. Like a mobile phone they are dependent on being in an area with sufficient signal.
Mobile Network	The infrastructure for carrying voice and/or data via radio waves to devices. When somebody says 'I can't get a signal' what they mean is they can't connect to the mobile network as the signal strength is not sufficient.
Mobile Phone	Refers to standard handset which typically does not have any 'advanced' capability (i.e. E-mail, Internet).
MobileIron / Airwatch / InTune	The MobileIron/Airwatch/InTune Virtual Smartphone Platform allows the trust to manage multiple operating systems at a granular level, provide mobile device management and securely support corporate devices, enforce cost control, and create a private enterprise application storefront for employees. It also gives the ICT Department the ability to utilise a device tracking function to locate/remote wipe a device if it is lost or stolen via location services.
Nebula Login/ Account	Nebula is the name of the Organisation provided computer network. When you log into your computer or laptop you are logging on to the Nebula network. Nebula's infrastructure provides your email and networked drive and print capability.
PCD	Personal Confidential Data (see Information Security Policy for detailed definition)

Term	Definition
Premium Rate	This refers to telephone numbers or SMS services which charge a higher price to contact them. Usually this is in order to provide a profit to the operator. Examples of premium rate services are voting on reality shows, competitions at the end of TV programmes or information services such as Weather or Traffic updates. Contacting such services on an Organisation provided device is prohibited, and so care should be taken as the profit motive of some operators leads to some unscrupulous practises.
RAS Token	A small device which generates an authentication code which gains access to the Organisations VPN network.
SIM only	This is a mobile data connection SIM card that is built within a laptop that has the ability to house this
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
Smart Phone	A mobile phone which also provides 'advanced' services such as E-Mail, Internet, Wi-Fi, GPS. Examples include, Apple iPhone, Android.
SMS	Short Message Service or more regularly known as a text/text message. A short message that a phone is able to receive or send. These are generally quite cheap, but it is possible to text Premium services which either create large subscription costs or cost more than the standard rate.
Tag Number	Most Organisation issued devices have a small sticker or 'tag' on them that contain a unique number that identifies the machine
Tethering	Refers to connecting one device to another. In the context of mobile phones or Internet tablets, tethering allows sharing the Internet connection of the phone or tablet with other devices such as laptops. Connection of the phone or tablet with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example through USB. If tethering is done over Wi-Fi, the feature may be branded as a Mobile Hotspot. The Internet-connected mobile device can thus act as a portable wireless access point and router for devices connected to it. This is breaking the Information *Security Policy* for the Organisation.
VPN Connection	A VPN, or Virtual Private Network, uses publicly available infrastructure such as the Internet to connect to a private network, in our case Nebula. The 'Virtual Private' refers to the use of technology to secure the link so that it is almost as secure as a private link.
Wi-Fi	This is the common term used to refer to a specific type of Wireless data connectivity. It is the most common form of wireless data connectivity and is used widely in people's homes and in public spaces such as Cafés or Hotels. Whilst bringing great freedom to computer usage they are prone to hacking and security breaches.

Terminology

Term	Meaning/Application
SHALL	This term is used to state a Mandatory requirement of this policy
SHOULD	This term is used to state a Recommended requirement of this policy
MAY	This term is used to state an Optional requirement

Implementation Plan

Development and Consultation	HBL ICT SMT Hertfordshire, Bedfordshire and Luton ICT Shared Services (HBL ICT) is committed to the fair treatment of all, regardless of age, colour, disability, ethnicity, gender, gender reassignment, nationality, race, religion or belief, responsibility for dependents, sexual orientation, trade union membership or non-membership, working patterns or any other personal characteristic This policy / procedure will be implemented consistently regardless of any such factors and all will be treated with dignity and respect. To this end, an equality impact assessment has been completed on this policy.
Dissemination	Staff can access this policy via the Intranet and will be notified of new/ revised versions via the staff briefing. This policy will be included in the ICB's Publication Scheme in compliance with the Freedom of Information Act (FOI) 2000
Training	Basic user documentation is provided to staff when they are given a specific device model for the first time. Use of Smart Phones and mobile data sticks allows for data to be stored on mobile devices. All members of staff using these are required to undergo basic Information Governance training as defined by the appropriate Governance department. For fixed Lines and IP Based Telephony services, all sites will have a main instruction manual and a variety of user manuals provided for end users.
Monitoring	HBL ICT is responsible for the day-to-day operation and monitoring of compliance with this policy. NHS Counter Fraud will become involved if a significant level of misuse is suspected. Managers of staff with devices covered by this policy must ensure that they keep track of the devices, including their return when the user no longer needs the device or leaves the organisation. The Partner via the Data Security and Protection Toolkit (DSPT provides the means by which the NHS and Partner can assess our compliance with current legislation, Government and National guidance
Review	The policy will be reviewed annually
Equality, Diversity and Privacy	Completed separately

References

External : Legislation, Guidance and Standards	All applicable UK Laws including o Data Protection Act and UK General Data Protection Regulation o Health and Safety at Work and Personal Safety o NHS wide Counter Fraud service policies and procedures o UK Law with regard to usage of mobiles in Vehicles o NHS Digital Good Practice Guidelines NHS Digital Telecommunications Example Policy V1.0
Internal : Related Documentation	Mobile Device Security Policy Information Security Policy Acceptable Use Policy Records Management & Information Lifecycle Management Policy (which includes Data Quality) (HWE ICB) Management of Records Policy and Procedure Data Quality Policy Information Governance Strategy Incident Policy Confidentiality Policy Standing Financial Instructions *ICT Purchasing Policy* *Health and Safety Policy* Mobile Device Request Form Change of User Form Returns Form
Enclosures	None

Contents

1 Executive Summary

This policy sets out the commitment of the Organisation to ensure that telephony services (outlined below) are adhered to in order to preserve the confidentiality, integrity and availability of all telecommunications.

The Policy aims to ensure that managers and staff are cognisant with the following areas:

- Management and use of telecommunications equipment.
- Financial and procurement regulations.
- Security and control of telecommunications equipment and all data stored within.
- Acceptable use of telecommunications equipment.
- Maintenance of privacy and dignity.

This policy applies to:

- Fixed line telecommunications platforms;
- IP telecommunications platforms;
- Mobile telecommunications;
- Mobile data connectivity contracts/PAYG delivering voice and/or data services (2G/3G/4G/5G).

Application of the policy will assist in compliance with the Organisation's Information Security Policy, information related legislation, NHS Information Security Standards and NHS Information Governance Standards.

This policy should be reviewed in conjunction with the *Mobile Device Security Policy*.

2 Introduction

This policy and procedures aim to address issues related to telecommunication devices and give clear guidance on the rules applying to their usage. It is the duty of all individuals issued with or using any telecommunication device provisioned by the organisation in accordance with the instructions and guiding principle given in this policy.

Budget Holders and Managers are responsible for ensuring members of staff conform to this policy. They are responsible for ensuring all members of staff are aware of the relevant policies and the need to follow them. They are responsible for reporting to the ICT department or local IG lead any concerns regarding adherence to this policy. Managers are required to monitor fair usage and take actions where necessary by reviewing their expenditure on telecommunication charges on monthly basis. This information should be provided to managers as part of their monthly management accounts.

3 Purpose and Scope

3.1 Who is eligible for a mobile device?

3.1.1 Mobile Phones/Smart Phone Devices

Mobile phones and Smart Phone devices are issued solely on the basis of need as determined by the budget holder ordering the mobile phone for the staff member. Managers are required to assess and authorise request for telecommunication device/s based on business need and eligibility.

Mobile telephones may be issued on an individual or shared basis. However the team manager will retain responsibility for such a phone if this is on a shared basis. All users of the device are bound by this policy.

3.1.2 Mobile Data Devices

In addition to the assessment and approval of the Budget holder as detailed above, Mobile Data Devices require additional security approval. This is carried out by HBL ICT on behalf of all the Partners it provides these services to.

3.2 Applying for a Mobile Device

The Purchase of all Mobile Devices must be in accordance with ICT recommendation and all devices remain the property of the Organisation at all times.

For Mobile Phones and mobile data sticks a ***Mobile Device Request Form*** must be completed via the online ordering system that is in place for the organisation. If this function is not yet available for your organisation, a hard copy of the form is to be completed and forwarded via email to the ICT department's Service Desk. The authoriser of the form is accountable for ensuring the accuracy of the details submitted, incomplete forms, or those where an inconsistency is identified will be returned with the requests not logged.

3.3 Acceptable Use

All employees are expected to use Organisation provided Mobile Devices in an appropriate manner. These devices are provided to allow the employee to carry out their work safely and efficiently. As such, no Mobile Device provided by the organisation should be used, loaned or given to anyone else - for example friends or family.

If a device is to be re-allocated to another member of organisation staff then this should be notified to the ICT department as otherwise the assigned user remains responsible for the unit and all costs associated with it. A copy of the ***Change of User Form*** needs to be completed accurately in full and forwarded by email to the ICT departments Service Desk. The authoriser of the form is accountable for ensuring the accuracy of the details submitted. Incomplete forms, or those where an inconsistency is identified will be returned with the requests not logged.

Acceptable use is considered to be the use of the device as a tool to carry out the task required by the user's employer. Equipment is provided for the conduct of official organisational business, limited personal use may be permitted at the discretion of the appropriate Senior Manager. Refer to Information Security Policy for further information

With regards to the telephone element, the following are examples of usage the organisation views as unacceptable:

- Calls/Texts to premium rate numbers, e.g. 0900 rate.
- Calls/Texts to vote on TV or Radio programmes e.g. X Factor.
- Calls/Texts to subscribe to services such as weather forecasts, horoscopes, etc.
- Calls/Texts to subscribe to Ring Tone/phone personalisation services.
- Calls/Texts to Adult services.

With regards to the data element of any Smart Phone/Mobile Device the following are examples of usage the organisation views as unacceptable:

- Using the Organisation data allowance allocated to a device for personal use i.e. accessing the internet, listening to music/ apps, games etc.
- Downloading non business related and charge attracting applications on smart phones
- Using any satellite navigation systems/apps on the device for assistance when driving as this is violating the organisation's *Health and Safety Policy*. This also uses a high amount of the devices data allowance.

Tethering your device to any other device (i.e. Laptop/other mobile device) to use the data connection for your mobile device must be done in accordance with the governing security policy.

This is not an exhaustive list; however it is indicative of examples of abuse which have been successfully pursued by organisation HR and Counter Fraud teams.

With regards to Smart Phones and Mobile data access, the user is governed by the same policies they accepted when they applied for a Nebula (network) login.

Please note all email and internet access from a mobile device is monitored in the same manner as from your desktop.

Failure to adhere with above requirements may result in disciplinary action and possibly a dismissal depending on severity of misuse.

3.3.1 Telephone Security

- The identity of the caller or person called **shall** be established prior to disclosure of any information. This will be the responsibility of the member of the organisation staff dealing with or making the telephone call.
- Identity **shall** be established in all cases, including where the call has been transferred internally.
- Where there is uncertainty over the genuineness of a caller, staff **shall** request the caller's telephone number, confirm its authenticity and call back. This return call **should** be made from another telephone where possible
- When a caller requests any information, staff **shall** verify the name, job title, department and organisation of the person requesting the information and the reason for the request. Staff **shall** consider whether it is appropriate and/or permitted for the information requested to be provided in response to a telephone request and in a telephone conversation. If in doubt, staff **should** consult their Line Manager.
- All staff **shall** ensure that there is no risk of telephone conversations being overheard by unauthorised persons.
- When making calls that are passed to voice mail systems, staff **shall** ensure that no information is recorded other than name of caller and return contact telephone number.
- Staff using IP telephones must make sure they have logged out after they have finished using the device especially in meeting rooms.

3.3.2 Use of Simple Message Service (SMS)

- Staff who use SMS or 'Text Messages' for valid business reasons **should** receive appropriate training and be made aware of expected SMS good practice, personal accountabilities and Information Governance (IG) requirements.
- Staff **should** avoid sending messages that could be deemed embarrassing or distressing, or that could be misinterpreted by the intended recipient.
- Staff **should** examine carefully any text messages received as these could contain errors. Word abbreviations and other acronyms are commonly used within SMS messages as a means to maximise message content within limited text space. However, abbreviations easily understood by the author may be prone to mistyping and misinterpretation by the recipient.
- Staff **should** delete messages from their mobile phones when they are no longer required. However, staff **should** consider potential IG requirements and legal obligations for the retention and storage of any message before deletion.
- Staff should ensure that personal MMS messages are avoided at all times. Any work related MMS are also dealt with IG requirements.

3.3.3 Fax Security

General

- Staff **shall** always consider whether the use of fax is the most appropriate method of sending and receiving information.
- Staff **shall** ensure that fax machines are located in a ‘Safe Haven’ or a secure environment.
- When using fax to transmit information, it **shall** be restricted to a minimum. Only information which is essential **should** be included in the information transmitted.
- Pre-programmed fax numbers **should** be regularly checked to confirm they are still valid.
- A speed-dial sheet showing the fax number and the organisation allocated to each of the speed-dial keys **should** be displayed next to the fax machines.

3.3.4 Sending by Fax

- Staff **shall** confirm that they have the correct fax number for the recipient.
- Staff **shall** take all reasonable steps to ensure that when a fax transmission is sent, it is received by the intended recipient.
- Staff **shall** confirm with the intended recipient that the receiving fax machine is located in a secure area or that the intended recipient is waiting by the fax machine to receive the transmission. Staff **shall** request confirmation of receipt of the fax by the recipient.
- The Organisation’s standard fax cover sheets **shall** be used with all fax transmissions. Cover sheets **should** show:
  - Sender’s name.
  - Sender’s telephone number.
  - Sender’s fax number.
  - Recipient’s name.
  - Recipient’s voice number.
  - Recipient’s fax number.
  - Transmission date and time.
  - Number of pages including the cover sheet.
- Staff **shall** ensure that cover sheets are not used to transmit information.
- Staff **shall** confirm by telephone that the intended recipient has received the transmission.
- Fax confirmation sheets **shall** be checked as soon as possible after transmission to confirm that the receiving fax number and number of sheets transmitted are correct.
- If anything appears wrong when transmitting a fax, the call **shall** be suspended immediately.
- If it becomes apparent that a fax has been sent to the wrong number, it **shall** be reported as an information security incident.

3.3.5 Receiving by Fax

- Staff **shall** ensure that documents are not left unattended at fax machines.
- Fax machines **should** be regularly checked for unexpected received faxes.
- Any incoming fax **shall** be handled as appropriate to its content.
- If a fax is received in error, staff **shall** immediately notify the sender and destroy the received fax by an approved method. The Organisation's management **should** be informed of the incident as soon as practicable and relevant Incident process initiated.
- A specific fax machine **should** be identified and isolated to receive faxes out of normal working hours. All other fax machines **should** be programmed to forward faxes to this machine.

3.4 Loss, Theft or Damage

When a user accepts an Organisation's mobile device provided by the organisation, they agree to the following responsibilities:

- To inform their line manager and HBL ICT as soon as possible.
- To follow the requirements and advice laid out in this policy and any other attendant documents.
- To keep a note of their mobile phone number and any tag number that refers to the equipment.
- To take all reasonable steps to care for the device including, for example, not dropping or throwing the device, not getting the device wet, not losing the device, etc.
- To only make business calls from a mobile phone if an organisation land-line is not available for use, unless specifically informed of arrangements such as free mobile to mobile calls.
- To follow the procedures below should the device become lost, stolen, damaged or faulty, and to reimburse the organisation for any financial loss caused by not doing so.
- To not use the device in situations where it unsafe to do so.
- Should the user be threatened and asked to hand over their mobile device, they will do so without argument and then report it to the Police and Service Desk as detailed below as soon as it is safe to do so.

3.5 General standards when using the device

- To not use the device in situations where it is inappropriate to do so. For example to take a call or send emails whilst dealing with a member of the public or in a meeting, unless of a critical nature.
- To ensure their voicemail box has a personal message giving their name, and an alternative contact number for use in an emergency - this is particularly important for clinical staff with public facing roles.
- When the user is to be on holiday/long term leave/sick they should ensure their voicemail reflects this and check their voice mail messages on a regular basis.

3.6 What to do in Case of Loss, Theft or Damage to a Mobile Device

If any employee loses or damages more than one handset in any 12 month period the organisation reserves the right to charge the employee the full replacement cost of subsequent handsets and other replacement costs.

Otherwise, the cost of replacing the mobile device will be charged to the budget holder as there is no insurance on handsets. Please keep in mind the replacement cost for a phone is often significantly higher than its initial purchase cost as there is no new connection subsidy.

In the event of a loss/theft the member of staff should:

- Report the incident to the ICT Service Desk.
- In the case of Loss or Theft report the incident to the local police station and obtain an incident number. Please report this to the Service Desk as soon as you have this.
- In the case of Loss or Theft out of Service Desk Hours* contact the Mobile Network to report the incident and ask for a bar to be put on the device. The incident must still be reported to the Service Desk in working hours.
- For any mobile device, the Service Desk will require the phone number or/and the Asset tag number.
- If the mobile device is lost/stolen on site the Service Desk will require the details of the Senior Officer or Site Manager.

3.7 Use in a Vehicle

It is illegal to drive whilst using a mobile phone or any other device that is not integral to the vehicle.

Some Devices have GPS Software built in. The organisation has chosen not to disable this as it allows users to plan routes and can be useful when walking to sites. However, the organisation does not permit the use of this (or any other) software whilst in a moving vehicle. Therefore Staff must safely stop their vehicle and turn off the engine to use any Mobile Device for any function, including answering calls. Failure to do so is an offence and therefore could lead to prosecution.

It is recommended that phones are turned off when driving (or turned to silent mode) to avoid being distracted at the wheel and kept safely in glove compartment or boot..

The organisation does not condone the use of personal hands free kits and as such does not supply them. The use of such kits with organisation provided equipment is forbidden whilst driving.

Where a vehicle has a fully fitted hands free kit, or a built in Bluetooth solution, the organisation advises all users to pull over before taking or making any calls on organisation provided equipment.

Users must not use any Text or Email facilities on their device whilst driving.

Due to the risk of theft, mobile devices should be kept out of sight while in the car. Where possible, the device must not be left unattended in cars, if this is unavoidable, the device must be out of sight and secured, the vehicle secured and steps taken to minimise time

The organisation may take disciplinary action against anyone found not to have complied with the above requirements.

3.8 Roaming Arrangements

Phones are initially barred against making international calls and roaming overseas.

This will only be removed for organisation use, and by agreement between the Budget Holder for the phone and the relevant Assistant Director. Seven (7) working days' notice is required when you log a call with the ICT Service Desk.

The international bar/roaming agreement will only be lifted temporarily - i.e. for the period such a facility is required.

International calls made to or from a mobile are expensive compared to a landline, and as such a landline should be used wherever possible. Individual calls should be approved by a manager or Assistant Director.

Before agreeing to remove international barring, consideration should be given to the great expense of making and receiving international calls. Additionally due to the loss of Caller ID data across international networks, it is impossible to trace many calls/ callers and as such impossible to determine personal use or abuse.

Smart Phones and 3G/4G/5G Data devices can very quickly generate huge costs as International Data Costs are high and are not regulated in anyway. It is also worth considering the increased security risk of using networks abroad which do not share similar UK security standards.

Due to *the Data Protection requirements* - Roaming will not be enabled as standard for use outside of the EU, if it is required, please contact the Service Desk for further advice.

3.9 Personal Mobile Data Devices

There is no requirement for staff to use their own personal phones for work purposes. As such there is no mechanism for claiming back the cost of calls made on a personal phone.

Staff should not give personal mobile phone numbers to patients.

Staff must not use Personal Smart Phones to connect to the organisations network, nor to save or store organisation related data without necessary checks being undertaken.

3.10 Privacy and Dignity

Mobile phones/Smart Phones with the capacity of taking photographs/videos can be useful for capturing information such as issues with buildings, describing locations, etc. However, images can represent a threat to the privacy and dignity of staff, service users and others and can be a breach of the *Data Protection Act* / UK GDPR and the *Human Rights Act*.

Photographs/Videos should only be used where this is a documented legitimate grounds for purpose approved by a Senior Manager and IG Manager from your organisation. The photographs must not include images of any people unless you have explicit consent from the individuals – you will need to be able to demonstrate that you will be handling the data fairly and lawfully.

Users should be aware of their surroundings when using a mobile phone, especially when discussing patient information.

Users should be aware that all usage of Mobile Devices is tracked and recorded. For example, numbers called/texted, duration of calls, times etc. This information is accessible by the ICT Department and may be provided to other appropriate departments if requested.

3.11 Pool/Group Phones

Where one (1) mobile device is to be shared within a team, the Team Leader/Manager is responsible for ensuring its appropriate use. It is their responsibility to keep a log detailing who had use of the device with times and dates to provide an audit trail.

There is no personal use, except in an emergency, and if the scenario arises, then the user must report the personal use to the responsible manager. The person responsible for the device is solely responsible for monitoring for any abuse or misuse.

3.12 Monitoring of Use

The use of Mobile Devices is monitored. Users should be aware their usage is not a private matter and, as such, use their device appropriately.

Staff may be asked to account for unusually high or expensive call levels and costs or unusual usage patterns. If these cannot be shown to be necessary and work related the user is liable for the full cost.

Usage information may be provided to the user's employing organisation for use in investigations or for other reasons deemed appropriate.

Usage information may be provided to external organisations, such as NHS Counter Fraud or the Police.

3.13 Malicious Calls

Mobile Devices are issued to enable effective and safe working practises. They should never be used for malicious reasons, to cause upset or bully.

If a user receives malicious or abusive calls or texts, they should report this immediately to the Service Desk.

If they feel it is appropriate, they should also contact the Police.

The Service Desk will provide further assistance. In the interim the user should not delete any text messages or delete any call logs as these can provide useful information in identifying the culprit - even if the number is withheld.

If need be, turn the device off.

3.14 Smart Phone Specific Information

Internet Access and Email from a Smart Phone is monitored in the same way as access from your desktop or laptop. The user is governed by the same rules they signed up for when applying for a Nebula login.

The following are forbidden:

- Access to web based Email services -Hotmail, Gmail, Yahoo, etc. These can more easily allow viruses onto the device.
- Access to social networking sites where this is against the organisations policy
- The downloading and storage of Personal Confidential Data on the unit without written express permission from your Director or the Caldicott Guardian.
- The downloading and storage of Organisation sensitive data.
- The removal of any password protection, management software (MobileIron/Airwatch) or turning off any location services or tracking functions on the device.

Should you require a specific app for work purposes, please make this request to the Service Desk for further investigation.

In addition, you must keep your Smartphone passwords secure and inform the Service Desk immediately if you feel it has become compromised.

Don’t write down your passwords and don’t keep it with the device.

You must safeguard all information on the device from loss, damage, corruption and unauthorised access or disclosure.

You must keep the Wireless Wi-Fi Data facility of a Smartphone disabled at all times, and not connect to any Wireless network - public or private - other than via a WPA2 encrypted connection. To do so compromises security of the data on your unit.

If you have a mobile device managed by the Airwatch or InTune platform then the Wi-Fi facility will be enabled and will connect automatically to the Wireless Access Points that sit on the organisations network.

You are able to connect the device to your own personal home Wi-Fi providing you are using WPA2 or better, encryption. Refer to the *Mobile Device Security Policy* for further information.

3.15 Mobile Data Specific Information

When provided with a laptop, you may also be provided with a RAS Token to gain access to the network via the secure VPN. This is the only connection you are permitted to make with your organisation issued Mobile device, i.e. you will be restricted from accessing the World Wide Web before connecting to the Nebula network.

You must keep your RAS Token safe. Do not write your PIN number on the RAS token as this will remove any element of security it provides. If you lose your RAS token you must report this to the Service Desk immediately.

3.16 Disposal of Mobile Devices

When ordering an organisation mobile device, the budget holder commits to a two (2) year contract. The relevant budget will be responsible for the phone and any associated accessories for this period. It may be possible in some cases to re-assign the device to another user; however this has to be with the agreement of all concerned. It is the budget holder’s responsibility to inform the ICT department when the device is no longer required.

If it is imperative to note that if a Mobile phone connection is cancelled within the two (2) year contract, the relevant budget code will be liable for all outstanding line rental costs, and any penalty charges.

Please complete the relevant Returns form available when you wish to dispose of a mobile device. The Device should be returned, with the *Returns Form*, and all its attendant accessories (e.g. battery, charger, SIM card, instructions, etc.) to the ICT Department.

The relevant budget will continue to be charged until all equipment is returned and until the end of the contract period, or until the device can be reallocated.

3.17 Transfer of a Smart Phone

If a member of staff is leaving the organisation and the smartphone is to be transferred to another member of staff, the Line Manager/Service Lead is required to ensure the smartphone is reset to factory default settings. This will then enable the smartphone to be ready for the next person. The Line Manager/Service Lead must ensure 'Find my Phone' option iPhone/iPad is **disabled before** the device is reset to factory default.

If the above process for removing Find my Phone and restoring the device to factory default has not been followed prior to returning the device for re-allocation, the Line Manager/Budget Holder will be responsible for the cost of replacing the device. The device cannot be unlocked via any other means if this has not been done.

Failure to inform HBL ICT of such changes may result in budget holder incurring additional cost.

4 Data Services

The organisation utilises a variety of mobile data services that provide 2G, 3G, 4G and 5G services from various carriers (Vodafone, EE). The delivery of data services can be split into two types; data services as part of Mobile/Smart Phone devices and data services used in dongles, Mi-Fi units, tablets and laptops.

There are varying factors which contribute to the quality, strength and availability of data/voice signal; these include proximity to a cell tower, physical obstructions such as buildings and network range and distance between cell towers.

Data Services which are delivered via dongle, Mi-Fi unit and directly connected to tablets and laptops will have additional security controls in place. Typically this is by the vendor 'locking down' the SIM cards so that they are unable to browse the internet unless connected to the corporate network via RAS. This helps to mitigate financial and reputational damage to the organisation in cases of lost, stolen devices.

5 Fixed Line/IP Telephony Systems

Fixed Line/IP Telephony within the organisation is predominantly provided via ISDN 2, ISDN30 and Analogue Lines, for use with MFD (Multi-Functional Devices), fax machines, franking machines, alarm lines, etc.

There are many feature sets that are in use on phone systems and these differ per site that you are on. The types of features are call routing / login-logout/voicemail, etc. The main reception for each site should have a hard copy of the phone system set up and common features in use on that site.

Premium numbers and International calling is centrally blocked on the phone systems, to protect the Organisations from unacceptable use. If these facilities are required for a particular service, then a call needs to be logged with the ICT Service Desk and this will be evaluated and if approved, will only then be set up. The ICT Department carry out ad hoc reviewing and reporting on bills, reporting any suspicious or excessive usage.

All support queries need to go via the ICT Service Desk

6 Exemptions

No members of staff using telecommunication devices provided by The ICT Department are exempted from the contents of this policy.

7 Accessibility considerations

Additional tools and features are available to staff who are using mobile and fixed telephony devices where required. These include (but are not limited to); accessibility features available on Android and iOS smart devices, bluetooth enabled peripherals and HAC comptaible handsets for fixed-line/IP telephony. Staff members should make their Line manager and the ICT team aware of accessibility requirements when requesting Telecoms equipment.

Appendix A. Comment Form

As part of HBL ICT Services Department continuous improvement regime, would you please complete this form. Any comments or feedback on this document should be addressed to the Owner. Please provide your name and contact details in case clarification is required.

Name Click here to enter text.

Address Click here to enter text.

Click here to enter text.

Phone Click here to enter text.

Email Click here to enter text.

Please return to:

HBL ICT Services
Charter House
Welwyn Garden City
Hertfordshire, AL8 6JL

Please confirm the document you want to give response to as:

HBL ICT Policy/Procedure: Click here to enter text.

Please rate the document using the topics and criteria indicated below:

	Very Good	Good	Average	Fair	Poor
Format and Layout	□	□	□	□	□
Accuracy	□	□	□	□	□
Clarity	□	□	□	□	□
Illustrations (tables, figures etc.)	□	□	□	□	□

When using the document, what were you looking for?

Click here to enter text.

How could the document be improved?

Click here to enter text.

How often do you use the document?

Click here to enter text.

If you have additional comments, please include them below:

Click here to enter text.

Thank you for your time.

Appendix B. Mobile Device Request form

The Request forms for new mobile devices are now available on the ServiceNow Customer portal:

Mobile Telecoms - ServiceDesk Portal (service-now.com)