NHS
Herts Valleys
Clinical Commissioning Group

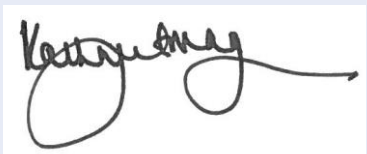
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		
Could this policy be incorporated within an existing policy?	No	
Does this policy follow the style and format of the agreed template?	Yes	
Has the front sheet been completed?	Yes	
Is there an appropriate review date?	Yes	
Does the contents page reflect the body of the document?	Yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	No	Policy about use of telecommunications
Are all appendices appropriate and/or applicable?	Yes	
Have all appropriate stakeholders been consulted?	Yes	
Has an Equality Impact Assessment been undertaken?	Yes	
Is there a clear plan for implementation?	Yes	Already in place as existing PCT policy
Has the document control sheet been completed?	Yes	
Are key references cited and supporting documents referenced?	Yes	
Does the document identify which Committee/Group will approve it?	Yes	

Plans for communicating policy to – staff; practice membership; public (as appropriate)	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Caroline Hall	Date	March 2018
Signature			

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Kathryn Magson	Date	March 2018
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

Telecommunications Policy

Version Number	2.0
Ratified By	Exec Team
Date Ratified	March 2018
Name of Originator/Author	Trudi Mount, Head of IM&T
Responsible Director	Caroline Hall
Staff Audience	All Staff
Date Issued	April 2018
Next Review Date	March 2019

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
0.1		First Draft	Mar 15	TLM
2.0		Amendments to revise usage of phones whilst driving Removal of HBL ICT policy	June 17	TLM

CONTENTS

1. INTRODUCTION

The Telecommunications Policy sets out the commitment of the CCG to ensure that telephony services made available in a manner that will preserve the confidentiality, integrity and availability of all telecommunications.

2. PURPOSE

The Policy aims to ensure that managers and staff are aware of the following areas:

- Management and use of telecommunications equipment
- Financial and procurement regulations
- Security 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 – e.g. iPhones
- Mobile data connectivity contracts/PAYG delivering voice and/or data services (2G/3G/4G) – e.g. iPads

Application of the policy will assist in compliance with the CCG'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.

3. DEFINITIONS

- Mobile Phone = Refers to standard handset which typically does not have any 'advanced' capability (i.e. E-mail, Internet)
- Smart Phone = A mobile phone which also provides 'advanced' services such as E-Mail, Internet, Wi-Fi, GPS. Examples include Blackberry, Apple iPhone, Android, Windows 8 Phone
- CSAR Form = The form a customer is required to submit in order to obtain a user account on the CCG's Nebula IT network. By signing the form the customer is agreeing to abide by CCG 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 = The Data Protection Act of 1998 is an act of the UK Parliament which defines the law in the UK for the storage, processing and transportation of data relating to identifiable living people. You are governed by it if 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.

- 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 rack up big subscription costs or cost more than the standard rate.

- MMS = Multimedia Message Service – similar to a SMS but extends its capability to allow the user to include photos, movie clips or other media content. They are more expensive than a normal SMS.

- 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 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 a CCG 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 = Also known as a 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.

- Sim only = This is a mobile data connection sim card that is built within a laptop that has the ability to house this.

- 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 Security Policy for the CCG.

- MobileIron = The MobileIron Virtual Smartphone Platform allows the CCG to manage multiple operating systems at a granular level, provide mobile device management and security support corporate devices, enforce cost control, and create a private enterprise application storefront for employees. It also gives the ICT Department the ability to utilize a device tracking function to locate/remote wipe a device if it is lost or stolen via location services.

- Location Services = Allows remote location-tracking of iOS devices mentioned above 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.

- Apple ID = A unique corporate/user ID used in creating an ITunes account for use with an Apple iOS device.

- Nebula Login/Account = Nebula is the name of the CCG 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.

- 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 a CCG 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 CCGs VPN network.

- VPN Connection = A VPN, or Virtual Private Network, uses publically 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 Cafes or Hotels. Whilst bringing great freedom to computer usage they are prone to hacking and security breaches.

- Tag Number = Most CCG issued devices have a small sticker or “tag” on them that contain a unique number that identifies the machine.

4. ROLES AND RESPONSIBILITIES

4.1. Roles and Responsibilities within the Organisation

All staff have a responsibility to act in compliance with this policy.

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.

4.2. Consultation and Communication with Stakeholders

This policy has been developed by the CCG’s ICT Provider in conjunction with the CCG Head of IM&T

5. CONTENT

Mobile Phones and increasingly Smart Phones are required by staff in order to carry out their work safely and efficiently. There are many benefits to the organisation in having Mobile Phones/Smart Phones available for staff use; however there are implications, costs and responsibilities, which require clarification.

This policy aims to address these issues and give clear guidance on the rules applying to the usage of provided Mobile Phones/Smart Phones.

It is the duty of all issued with or using a CCG Mobile Phone/Smart Phone to comply with and follow the instructions given in this policy.

The HBL ICT Shared Service are responsible for providing prompt assistance to all users and other Stakeholders, in accordance with the CCG's Service Level Agreements (SLA's). They are responsible for monitoring usage and reporting unusual usage patterns or other indications of abuse to the relevant bodies.

5.1. Who is Eligible for a Mobile Device?

5.1.1. Mobile phones/Smart Phone Devices

Mobile phones and Smart Phone devices are issued solely on the basis of need as determined by their line manager.

5.1.2. 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 the ICT department on behalf of all the organisations it offers these services to.

5.2. Applying for a Mobile Device

The Purchase of all Mobile Devices must be in accordance with ICT's purchasing policy and all devices remain the property of the CCG at all times.

All devices will be ordered in line with the CCG ordering process and be processed via Corporate Services.

5.3. Acceptable Use

All employees are expected to use CCG 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 CCG should be used, loaned or given to anyone else – for example friends or family.

Any reallocation of devices must be done by the CCG Corporate Support Team who will inform ICT of such changes.

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. Personal use is acceptable in limited circumstances as set out in this policy. Otherwise, unacceptable use will be regarded as noncompliance of this policy.

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

- Using the CCG data allowance allocated to a device for personal use i.e. accessing the internet, listening to music/ apps, games etc. Using the device for personal use whilst connected to free Wi-Fi, and thus is not incurring charges, is acceptable providing such use does not contravene any other guidance such as security policies.
- Tethering your device to any other device (ie. Laptop / other mobile device) to use the data connection for your mobile device unless absolutely necessary. This also uses a high amount of the devices data allowance,

This is not an exhaustive list; however it is indicative of examples of abuse which have been successfully pursued by 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 login.

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

5.4. Loss, Theft, Damage

When a user accepts a CCG provided mobile device, they agree to the following responsibilities:

- 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.
- Where possible staff are asked to make business calls from a mobile phone if a CCG 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 CCG for any financial loss caused by not doing so.

- To not use the device in situations where it unsafe to do so.

- 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.

- 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.

- 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.

5.5. 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 CCG reserves the right to charge the employee the full replacement cost of subsequent handsets and other replacement costs, depending upon circumstances.

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 (see useful contacts) 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.

5.6. 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. Managers should not expect or encourage staff to answer calls when driving and all CCG employees are reminded of the government guidance on this:-

It is illegal to use your phone while driving or riding a motorcycle unless you have hands-free access, such as:

- *a bluetooth headset*
- *voice command*
- *a dashboard holder*

The law still applies to you if you're:

- *stopped at traffic lights*
- *queuing in traffic*
- *supervising a learner driver*

Hands-free

The CCG does not condone the use of personal hands free kits and therefore does not supply them. Where a vehicle has a fully fitted hands free kit, or a built in Bluetooth solution, users should pull over before taking or making any calls, to ensure their own safety and that of other road users.

When you can use a hand-held phone

You can use a hand-held phone if either of these apply:

- *you're safely parked*
- *you need to call 999 or 112 in an emergency and it's unsafe or impractical to stop*

Penalties

You can get 6 penalty points and a £200 fine if you use a hand-held phone.

You can also be taken to court where you can:

- *be banned from driving or riding*

- *get a maximum fine of £1,000 (£2,500 if you're driving a lorry or bus)*

If you passed your driving test in the last 2 years, you'll lose your licence.

Some Devices have GPS Software built in. The CCG has chosen not to disable this as it allows users to plan routes and can be useful when going to sites.

Due to the risk of theft, mobile devices should not be left unattended in cars at any time. They must also be kept out of sight while in the car.

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

5.7. Roaming Arrangements

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

This will only be removed for CCG use, and by agreement between the budget holder for the phone and the relevant Assistant Director. Seven 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.

Due to Article 8 of the Data Protection Act it is not possible to enable Roaming for use outside of the EU. In such cases please contact the Service Desk for further advice.

5.8. Personal Mobile Data Devices

There is no mechanism for claiming back the cost of calls made on a personal phone for work purposes.

Staff should not give personal mobile phone numbers to patients/clients.

Staff must not use Personal Smart Phones or BlackBerrys to connect to the CCGs network, nor to save or store CCG related data.

5.9. 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 and the Human Rights Act.

Therefore, it is forbidden to use such devices to photograph people in the workplace unless you have their permission. Photographs/Videos should only be used rarely where this is a justified and approved purpose, and these should not include the images of any other people unless you have their permission. It is particularly important that express permission is obtained when photographing/videoing non CCG employees.

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

5.10. 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.

5.11. 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.

5.12. Smart Phone Specific Information

Internet Access and Email from a Smart Phone is monitored in the same way as access from your desktop. 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 allow viruses onto the device.
- Access to social networking sites – Facebook, Myspace, Bebo, etc. The exception to this is where sites are utilised by the CCG for work purposes e.g. Yammer.
- The downloading and storage of Personal Confidential Data on the unit without written express permission from your Director or the Caldecott Guardian.
- The downloading and storage of CCG sensitive data.
- The removal of any password protection, management software (MobileIron) or turning off any location services or tracking functions on the device.

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.

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

You are able to connect the device to your own personal home Wi-Fi providing you are using WPA2 or better, encryption; however you MUST NOT connect to any public Wi-Fi hotspots, as this would be classed as a security breach.

Refer to the CCGs Mobile Device Security Policy for other related procedures

5.13. 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 CCG 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.

5.14. Disposal of Mobile Devices

When ordering a CCG mobile device, the budget holder commits to a two-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 that a Mobile is cancelled within the two-year contract, the relevant budget code will be liable for all outstanding line rental costs, and any penalty charges.

Corporate Services will manage the purchasing and disposal of all mobile devices.

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.

5.15. Fixed Line / IP Telephony Systems

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.

Premium numbers and International calling is centrally blocked on the phone systems, to protect the CCGs for 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 Network and Telecommunications Team carry out ad hoc reviewing and reporting on bills, reporting any suspicious or excessive usage.

6. MONITORING COMPLIANCE

This policy will be reviewed annually in line with the CCG ICT Provider policy refresh. The policy is the responsibility of the CCG Head of IM&T.

The HBL ICT Network and Telecoms Manager is responsible for the day to day operation and monitoring of compliance with this policy.

NHS Counter Fraud will be become involved if a significant level of abuse 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.

7. EDUCATION AND TRAINING

Basic user documentation is provided to staff when they are given a specific device model for the first time.

Use of BlackBerrys/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 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.

8. REFERENCES

N/A

9. ASSOCIATED DOCUMENTATION

Standing Financial Instructions

Information Security Policy

Guidance on the use of E-Mail when sending PCD

Mobile Device Security Policy

Information Governance Strategy

Incident Policy

Confidentiality Policy

Health and Safety at Work and Personal Safety

NHS wide Counter Fraud service policies and procedures

UK Law with regard to usage of mobiles in Vehicles

Data Protection Act

All applicable UK and EU Laws

APPENDICES

10. Appendix A

Acronyms

NHS = National Health Service

CCG = Clinical Commissioning Group

IT = Information Technology

ICT = Information and Communications Technology

IM&T = Information Management and Technology

EU = European Union

SIRO = Senior Information Risk Owner

DH = Department of Health

UK = United Kingdom

PCs = Personal Computers

HSCIC = Health and Social Care Information Centre

PCD = Personal Confidential Data

Appendix C - Equality Analysis - Equality Impact Assessment Screening Form

Name of policy / service	Telecommunications policy
What is it that is being proposed?	This policy seeks to define rules to cover the use of corporate mobile devices for corporate use
What are the intended outcome(s) of the proposal	The outcome of the proposal is to define a set of rules governing the use of HVCCG devices for corporate purposes.
Explain why you think a full Equality Impact Assessment is not needed	This is a policy creating guidance for use of devices and is equally applicable to all staff
On what evidence/information have you based your decision?	The policy is relevant to all staff of all levels
How will you monitor the impact of policy or service?	N/A
How will you report your findings?	N/A

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.	
Assessors Name and Job title Date	Trudi Mount Head of IM&T 12th October 2017