NCL Clinical Commissioning Group's ICT Equipment: Acceptable Use Policy V0.2

January 2020

Contents

1. Introduction

This policy applies to the NHS Barnet CCG, NHS Camden CCG, NHS Enfield CCG, NHS Haringey CCG and NHS Islington CCG, hereafter referred to as NCL CCG's.

The use of computing and telephony devices, and access to systems and information from a variety of NCL CCG's sites, customer sites and remote locations is fundamental to the efficient operation of the NCL CCG's. Computing and advanced telephony brings many benefits, allowing information to be made available from any location, whilst working on the move, in remote offices, on client sites or from home.

Much of the information held by NCL CCG's is confidential and/or business sensitive. Mobile, remote and home working carries more risk of a breach in security than in a controlled office environment, whether it is personal information held on laptops, contact details on a mobile phone or a financial spread sheet emailed to a personal account, the risks to information are obvious.

It is essential that these risks are identified and appropriate risk-mitigating controls implemented to ensure robust information security arrangements. The NCL CCG's policy on the use of these technologies are set out in this policy and apply wherever information is remotely accessed from devices that are not located on NCL CCG's premises. The devices may be provided by NCL CCG's, owned by staff, provided by third-party employers, or other.

2. Objective

This policy is linked to the Information Security Policy and the operational/technical policies of NCL CCG's in the provision of the ICT service.

The purpose of this policy is to provide guidance to staff on acceptable standards of access and use of NCL CCG's information and systems, whether within the main office or from remote locations using mobile devices.

It defines acceptable use while working for or with NCL CCG's in relation to:

- Responsibilities and use of ICT assets
- Use of email and internet
- Network use
- Office-based use
- Remote use, including via wireless internet, 3/4G, Bluetooth and global positioning system (GPS)

In the context of this policy, mobile computing is a term used to describe the use of mobile and data bearing devices that process NCL CCG's data. This will include items such as:

- Laptops
- Removable media (DVD/CD, memory sticks, memory cards, external hard drives)
- Mobile phones
- Smartphones
- Tablets
- Personal digital assistants (PDA)
- Digital cameras
- Video cameras

- Webcams
- Dictation devices
- Digipens
- E-readers

NCL CCG's has statutory duties in respect of data, information, ICT Security and Records Management. It also has a duty to comply with guidance issued by the Department of Health and NHS, including NHS England and NHS Digital.

Centrally provided NHS applications (e.g. SBS and NHSmail) are subject to the NHS terms and conditions of use and their Acceptable Use Policy.

3. Scope

This policy applies equally to all staff who are directly employed by NCL CCG's and to those for whom NCL CCG's has legal responsibility, i.e. contractors and consultants. The NCL CCG's policies are also applicable to those staff in other forms of employment – such as honorary contract or work experience – whilst undertaking duties for, or on behalf of, NCL CCG's. Further, this policy applies to all third parties and others authorised to undertake work on behalf of NCL CCG's.

4. Equality Analysis

This document demonstrates the organisation's commitment to create a positive culture of respect for all individuals, including staff, patients, their families and carers as well as community partners. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to use the Human Rights Act 1998 and to promote positive practice and value the diversity of all individuals and communities.

5. Duties and responsibilities

The Director of ICT has overall responsibility for procedural documents across the organisation; this includes establishing and maintaining an effective document management system, meeting all statutory requirements and adhering to guidance.

The NCL CCG's Information Governance (IG) Team will provide IG advice and guidance in line with contractual obligations and support ICT management where applicable.
Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy/strategy and procedure manuals
- Line managers
- Specific training courses
- Other communication methods (including team meetings)
- Intranet

6. General principles

All data and information on information systems managed by NCL CCG's remain the property of the CCG's at all times, unless explicitly otherwise stated in documented contracts for both staff and third party providers of services.

Access to the internet is provided for business purposes. Occasional and reasonable personal use is permitted (e.g. during lunch breaks), provided that such use does not interfere with performance of duties and does not conflict with NCL CCG's policies, procedure and contracts of employment.

Non-business related, or 'personal' use of NCL CCG's information systems is not a right and requires authorisation from the responsible manager; it must be exercised with discretion and moderation. NCL CCG's will not accept any liability, in part or whole, for any claims arising out of personal use of these systems or of the CCG's information.

NCL CCG's senior management retains the right to:

- require monitoring reports of the use of its information systems for the purpose of protecting legitimate concerns.
- prohibit personal use of information systems without warning or consultation –
- collectively, where evidence points to a risk to the CCG's and/or constituent businesses, or individually where evidence points to a breach of this or any other NCL CCG's or NHS policy.

7. User obligations

- Users must adhere to information classification procedures and information encryption requirements when sharing or sending NCL CCG's information, internally or externally.
- Users must follow established procedures for password changes and are forbidden to share their own, or other people's, usernames or passwords to gain access to any NCL CCG's or other information systems. Passwords must not be written down.
- All users must follow Health and Safety guidelines when using information systems.
- Users must comply with Copyright, Design and Patent Laws at all times, when downloading material from internet sites.
- It is mandatory for all users to lock their desktop computer, laptops, tablet or smartphone when not in use or they are away from their desk. For desktop computers and laptops this is done by pressing ctrl/alt/del (or 'windows key' and L).
- Tablets and/or smartphones must be locked to require a code for access whenever the device is not in use, even for short periods.
- Staff and ICT users will not be permitted to use their personal devices to connect to a NCL CCG's corporate network.
- Connection of personal devices to the NCL CCG's corporate domain is not permitted.

8. Prohibited and unacceptable use

Staff with questions about what is considered inappropriate use must check with their line manager or the IT Service Desk. Known sites falling within the above categories may be blocked by web security software or reported on access. If access is required to a site that is being blocked by the web security software, contact the relevant ICT service desk.

8.1 Prohibited use

Access to systems, including internet-browsing history is monitored. Monitoring information may be used to support disciplinary action. Sites deemed inappropriate are those with material that is defamatory, pornographic, sexist, racist, online gambling, terrorism and/or such sites whose publication is illegal or risks causing offence.

Anyone found to have been using the internet inappropriately may be disciplined and/or prosecuted. The following uses of the internet are strictly forbidden at all times:

- **Pornography:** this is banned in the workplace and is subject to disciplinary action.
- Accessing, uploading or downloading child pornography is illegal and the user will be reported to the police.
- **Illegal activities:** this includes, but is not limited to, sites promoting violence, racial discrimination or sexual harassment, sites that are defamatory or that are intended to harass or intimidate other staff.
- **Commercial activities:** this includes using NHS resources to operate a business or to sell online.
- **Activities for financial gain:** this includes, but is not limited to, lotteries and gambling.
- **Downloading material protected by copyright:** use must have express permission given in line with the *Copyright Designs and Patents Act 1988*.
- **Telephony:** No permitted access to premium rate calls and international roaming unless specifically authorised by a senior line manager.
- **Hacking:** breaking into other computer systems using the N3 network or internet.
- **Fraud:** providing false details or attempting to gain profit illegally.

Staff must be aware that it may be a disciplinary offence to make disparaging remarks about their employer, patients or other employees even when using their own computer at home on social networking sites including, but not limited to, Facebook, Twitter or LinkedIn.

NCL CCG's require all employees to be treated with dignity at work, free from harassment and bullying of any kind. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by email. Staff must not send any messages containing such material. Bullying and harassment of this kind will be treated as a serious disciplinary matter which may lead to dismissal.

8.2 Unacceptable use

Users are strictly prohibited from using NCL CCG's information systems and information in a manner that will:

- break the law and/or have legal implications or incur any liability to the CCG's and/or constituent businesses
- cause damage or disruption to the CCG's information systems
- violate any provision set out in this policy or any other policy
- contravene the NCL CCG's Code of Conduct
- waste time, decrease productivity or prevent the user from performing their primary responsibilities for the CCG's.

Users are not permitted to access any information to which they have not been given explicit authorised access. Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not given explicit access or authorisation.

Users are strictly prohibited from installing software on their NCL CCG's or other NHS supplied device. This includes the illegal download, copying and/or storage of copyrighted content onto the CCG's information systems.

Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website, the user must immediately inform their line manager or the ICT Service Desk.

Financial transactions are not permitted on websites requiring software to be downloaded prior to the transaction being executed. NCL CCG's accepts no responsibility for any charges and/or losses incurred in relation to personal purchases or personal transactions using the CCG's information systems regardless of cause. Only NCL CCG's approved standard and supported software for web conferencing and collaborative working must be used.

9. Mobile working

Staff issued with mobile computing devices including – but not limited to – those listed in Section 2, must ensure that the equipment is secure at all times.

Users of mobile computing devices must not allow unauthorised access by third parties including, but not limited to, family and friends.

9.1 General rules when using a mobile device

- All mobile devices must be operated in a secure manner at all times
- They must be kept in a secure place when not in use
- Equipment must not be left on office desks overnight
- Devices must not be left in a visible position in an unattended vehicles
- Devices must not be left in vehicles overnight or for long periods of time
- Devices brought in to a secure environment should be securely stored separately to other confidential information, especially papers
- The amount of information that is kept on the device must be kept to a minimum.
- All information must be stored on NCL CCG's network folders where it is regularly backed up, not locally on the device.
- Details of any password or PIN must be kept secure and separate from the device they access.

9.2 Rules for specific devices

9.2.1 Laptops

- All laptops must be encrypted to the level approved by the NCL CCG's ICT Department.
- Access to local administration level privileges is limited to approved NCL CCG's ICT Department technical staff to prevent the loading of unauthorised software or attempts to bypass security controls.
- All laptops must be connected to the network at least once each month, to enable the automated update of antivirus software and other security features.

- There are circumstances in which normal use prohibits the operation of some of the above controls. In these cases, the owner of the laptop may apply to the NCL CCG's ICT Department for approval.
- Use of remote connectivity is for business use only; for example – but not limited to – 3/4G, Bluetooth and tethering. Any other use may be charged to the member of staff proportionate to the type of use and type of connectivity.

9.2.2 Memory sticks/external hard drives/memory cards

- NCL CCG's provides memory sticks which meet the NHS encryption standards.
- Continued use of USB memory sticks will be periodically reviewed as the cost and availability of devices changes.
- All USB memory sticks used for the writing of information from NCL CCG's infrastructure must be encrypted to NHS standards.
- The writing of information to unapproved memory sticks is prohibited and will be prevented by the use of control software.
- Where no other means of transfer is possible, the transfer of information from any USB memory stick for processing on any NCL CCG's Desktop computer or laptop can be permitted for a limited time; once this process is complete the data must be appropriately deleted from the USB stick.
- the USB port will only allow the use of approved encrypted USB memory sticks.

9.2.3 Other removable media

- The use of other removable media, such as CDs and DVDs, for the writing of information is actively prevented, other than for the approved transfer of data for authorised purposes.
- Any such removable media must be encrypted if they contain confidential information.

9.2.4 Mobile phones

- All mobile telephones must be protected by a PIN that prevents the SIM card, the device and voicemail from being accessed by unauthorised users. Each of these must be separate and different PINs.
- Failure to enter the correct PINs will result in the device being locked after a certain number of failed attempts.
- Where hotspot tethering (i.e. the sharing of internet connections, in or out, between mobile tablets and other devices such as laptops) is authorised for some users, its use is strictly limited and only for business purposes.
- Mobile phones provided by NCL CCG's must only be used for business purposes. Any other use may be charged to the member of staff proportionate to the type of use and type of connectivity. Exceptions are for emergency use only, e.g. to call emergency services.

9.2.5 Smartphones and tablet devices

- All smartphones and tablet devices must be protected from unauthorised access by a PIN, password or other access control system.
- Failure to enter the correct PIN, password or other access control system will result in the device being locked and may result in all data being deleted.

- Downloading of unapproved applications or utilities is prohibited; systems may be put in place to identify devices containing unauthorised software.
- The same rules apply for tethering, as with mobile phones, above.
- Apps (i.e. computer programs designed to run on smartphones and tablets) should not be downloaded unless NCL CCG's has approved and authorised them for business use.
- Smartphones and tablet devices must only be used for business purposes. Any other use may be charged to the member of staff proportionate to the type of use and type of connectivity.
- Smartphones and tablet devices must have up-to-date software loaded (via Wi-Fi or 3/4G connectivity) to ensure the operating system is working to an appropriate security standard.
- Personal smartphones and tablets and/or apps on them must not be used to photograph, video or record any personal confidential data or business information.

9.2.6 Personal digital assistants

- NCL CCG's only permits the connection of a limited range of personal digital assistants (PDAs) to the network. PDA technology has largely been superseded by smartphone and tablet devices. New PDA devices will be supported only in exceptional circumstances.
- PDA devices must be protected by a PIN. The device is disabled or set to factory settings after a number of failed attempts.
- Encryption by the NCL CCG's approved method must be employed.

9.2.7 Digital cameras, video cameras and webcams

- Some NCL CCG's services may film or photograph patient activity for therapeutic reasons. The images are classed as confidential information for purposes of data protection. No filming can be carried out unless the patient has given their consent, either in writing or appropriately recorded by a health care professional.
- Internal (non-removable) storage must be used to store images/video where this is made possible by the device.
- Any removable media containing patient images must be marked as confidential where the physical size of the device permit this.
- Devices must be kept secure at all times.
- When not in use, all devices must be locked in a secure place; they must never be left in a visible position in an unattended vehicle.
- The amount of information that is kept on the device must be kept to a minimum.
- Images/videos must be copied to NCL CCG's network storage areas at the earliest opportunity and then deleted from the device.
- Devices must be used only for business purposes.

9.2.8 Dictation devices

- Handheld digital dictation devices have generally replaced analogue, cassette machines within NCL CCG's. Many of these machines are used for recording meetings to facilitate accurate minutes, the dictation of patient notes and/or other confidential information.
- NCL CCG's maintains a list of approved encrypted dictation devices. This list will be reviewed periodically as availability changes. Only encrypted devices may be purchased. Continued use of existing non-encrypted devices must cease.

- Unencrypted devices must be secured in the same way as digital camera, video camera and webcams (see above).

9.2.9 Digipens

- Digipens or smart pens are electronic devices that convert the written word to electronic documents automatically; some may also record audio and synchronise sound to written documents.
- Only approved digipen solutions may be used. Exceptions may be made under certain circumstances to enable staff with accessibility issues to work more effectively. This would require the authorisation of the IG and ICT Security and Compliance teams.

9.2.10 E-readers

- E-readers allow electronic documents to be read from small portable devices.
- Only devices approved by the NCL CCG's ICT Department can be used to store the CCG's documents.
- Personal devices must not be used to store NCL CCG's documents under any circumstances.
- Devices must be encrypted and kept in a secure location when not in use.

9.3 Loss or theft of mobile devices

- Any device that has been lost or stolen must be reported to the NCL CCG's IG lead and the NCL CCG's ICT Department as soon as possible.
- An incident report must be submitted detailing any confidential or sensitive data that may have been stored on the device.
- Where appropriate, the police must be informed immediately by the device holder.

10. Remote access to systems

Remote access to NCL CCG's systems can be provided using a number of technologies, including Citrix and VPN. These methods may vary as technological change occurs. Remote access may involve an upfront and/or on-going charge to your service.

- Unless by authorised exception, data must never leave the CCG's systems.
- Only NCL CCG's approved remote access methods can be used to allow remote working.
- NCL CCG's data must never be copied to personal devices.

10.1 Handling information

- Remote access to the NCL CCG's network may require two-factor authentication to ensure the security of the system.
- Confidential data must not be emailed to or from a home email account or personal email account. NHSmail provides the only solution for this.
- Access to NHSmail on a home computer must be in accordance with the NHSmail Acceptable Use Policy.

- Staff must not download any attachments to their home desktop computer or other device.
- Staff must ensure that NCL CCG's information cannot be accessed or viewed by members of their family/visitors.
- Extra care must be taken if access is taking place on a public computer or when using a personal or NCL CCG's provided device in a public area to ensure that unauthorised individuals are not able to access the CCG's systems or view on-screen data. The user must ensure that all systems are fully logged out and closed down before leaving a public machine unattended.
- The computer must never be left unattended whilst it is connected to NHS information.

10.2 Cancelling remote access

- It is the responsibility of authorising managers to revoke access to remote access systems when they are no longer needed.
- Charges will not be refunded if a manager has failed to revoke access in a timely manner.
- It is the responsibility of the authorising managers to ensure that remote access is disabled for any staff member currently suspended from duty

11. Tariffs for use of equipment and mobile technology

The tariffs for the use of equipment and mobile technology, which may be charged to users, as detailed above, are as described in this policy wherever a charge to an individual could be enforced. NCL CCG's will meet all other associated costs.

12. Monitoring arrangements

Users of the internet must be aware that each site they visit is recorded and that logs of sites are regularly examined to ensure inappropriate use is dealt with. A full security audit trail is maintained of records/sites accessed.

12.1 Compliance

Compliance with this policy will be monitored through the ICT Security Group which reports to the ICT Steering Group.

12.2 Non Compliance

12.2.1 Failure to comply with the standards and appropriate governance of information as detailed in this policy may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for

12.2.2 Failure to maintain these standards can result in HR disciplinary processes being followed which could result in criminal proceedings against individuals or the organisation

.

12.2.3 NCL CCG's reserves the right to amend this Policy without notice. If any changes affect the way staff use the ICT services and information assets, the CCG's will ensure that members of staff are informed and allowed a reasonable time for the changes to be implemented.

13. Review

This policy will be reviewed annually by the NCL CCG's, and in accordance with the following, on an as required basis:
Legislative changes

- Good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities
- Changes to organisational changes

Review will take place on the first anniversary of adoption and then subsequent approval will take place every three years until rescinded or superseded.