NHS
Haringey
Clinical Commissioning Group

Information Security Policy

1	**SUMMARY**	This Policy is designed to set the standards expected in order to maintain the security of information within the organisation, by ensuring a safe and secure environment for the Information held both manually and electronically.			
2	**RESPONSIBLE PERSON:**	Steve Beeho, Head of Integrated Governance			
3	**ACCOUNTABLE DIRECTOR:**	Jennie Williams, Executive Nurse and Director of Quality and Integrated Governance			
4	**APPLIES TO:**	All staff in Haringey CCG. Governing Body Members Third parties.			
5	**GROUPS/ INDIVIDUALS WHO HAVE OVERSEEN THE DEVELOPMENT OF THIS POLICY:**	NEL CSU Information Governance Team Jennie Williams, Executive Nurse and Director of Quality and Integrated Governance Steve Beeho, Head of Integrated Governance			
6	**GROUPS WHICH WERE CONSULTED AND HAVE GIVEN APPROVAL:**	Haringey CCG Senior Management Team. Haringey CCG Quality Committee.			
7	**EQUALITY IMPACT ANALYSIS COMPLETED:**	**Policy Screened** Yes		**Template completed** Yes	

8	**RATIFYING COMMITTEE(S) & DATE OF FINAL APPROVAL:**	Quality Committee (via Chair's Action) – 13.3.15			
9	**VERSION:**	2.2			
10	**AVAILABLE ON:**	**Intranet** Yes		**Website** Yes	
11	**RELATED DOCUMENTS:**	Information Governance Policy (2015) Confidentiality and Disclosure of Information Policy (2015) Calendar, Email and Internet Policy (2015) Information Management Policy (2015) Incident and Serious Incident Policy (2014)Information Governance Strategy and Framework (2015)			
12	**DISSEMINATED TO:**	All staff in Haringey CCG.			
13	**DATE OF IMPLEMENTATION:**	18.12.15			
14	**DATE OF NEXT FORMAL REVIEW:**	December 2017			

DOCUMENT CONTROL

Date	Version	Action	Amendments
9.9.13	1.0	First draft	
12.9.13	1.1	Second draft	Following feedback from SMT
22.10.14	1.2	Draft	Annual review.
23.2.15	1.3	Second draft	Key changes made to data/information classifications in section 6.4 and throughout the policy for consistency.
16.3.15	2.0	Revised	Amended to reflect that the policy has now been approved via Chair's Action.
4.11.15	2.1	Reviewed/updated	Internal and External Reporting of Incidents and Risk section in 6.5 updated to reflect changes made to HSCIC IG SI guidance IT helpdesk email updated Updated link to NHS Care Record Guarantee HSCIC Checklist Incident Reporting Guidance updated Service Level Agreements referenced as an alternative to contracts where applicable Proposal for a 2 year revision to this policy unless there are significant changes in legislation or national guidance which warrant an earlier review

CONTENTS

1. Introduction

The CCG will hold and manage some personal and confidential data relating to patients, the public and its employees. With ever-easier ways by which information can be accessed and shared it is important that a consistent approach is adopted to safeguard the organisation information as an asset.

This Policy is designed to set the standards expected in order to maintain the security of information within the organisation. Its adoption will ensure a safe and secure environment for the information held both manually and electronically and in particular that this information is operated in accordance within NHS guidance, Information Governance principles, ISO27001 security Standards, Caldicott Guidance and relevant legislation.

It will embed the concept of identifying, recording and managing Information Assets and associated risk within the wider risk management framework. It is intended to:

- Ensure identification and safeguarding of information assets;
- Link to the wider organisational risk management framework, in which information risks will be identified, considered and addressed in key approval, review and control processes;
- Meet contractual and legal requirements;
- Meet standards set through internal and external assessment obligations
- Meet the standards set within the NHS Operating Framework, NHS Constitution and NHS Care record guarantee.

Failure by any employee of the organisation to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary and/or legal action.

2. Policies statement

Haringey Clinical Commissioning Group (CCG) has put this policy in place to ensure staff are fully aware of their information security responsibilities. This policy is important as it should help you understand how to look effectively maintain the security of the information needed to do your jobs consistent with the law and expected standards.

Information is a valuable asset to a commissioning organisation to enable it to effectively make informed decisions. Therefore it is important to ensure we maximise the value of information as an ‘asset’ in compliance with legal requirements. To do this we will ensure information is:

- **H**eld securely and confidentially;
- **O**btained fairly and lawfully;
- **R**ecorded accurately and reliably;
- **U**sed effectively and ethically; and
- **S**hared and disclosed appropriately and lawfully.

The CCG is committed to ensuring that information, in whatever its context, is processed as determined by prevailing law, statute and best practice. Compliance with all organisation

policies is a condition of employment and a breach of policy may result in disciplinary action.

3. Scope of this policy

This policy covers all aspects of security when holding, obtaining, recording, using, sharing and disclosing of data/information or records, held in a manual/paper or electronic format, by or on behalf of the CCG.

This includes, but is not limited to; staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

4. Purpose

The Policy is intended to achieve and maintain the following Information Governance objectives:

Confidentiality
Assuring that sensitive information or data is accessible to only authorised individuals, and is not disclosed to unauthorised individuals or the public unless appropriate and lawful.
Integrity
Safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.
Availability
Ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.
Accountability
Users will be aware of their responsibilities in relation to their collection, use and processing of data and information.

5. Who this policy applies to: Roles and responsibilities

Security is everybody's business and therefore it is everybody’s responsibility to ensure information is secure. This section describes the expected responsibilities in relation to Information Security of persons processing information. It is noted that some individuals will hold more than one role.

Role	Responsibilities
Governing Body	In line with the Guidance for NHS Boards: Information Governance, the governing body will ensure that its organisation has taken appropriate steps to meet IG standards. In particular it will seek assurance against following questions: 1. "What have we done, as an organisation, to ensure we have implemented adequate policies and procedures, and are addressing the responsibilities and key actions required to support effective IG?" 2. "What were the outcomes of our most recent annual IG assessment, and what measures (if any) have been put in place to address any identified deficiencies?" 3. "What plans do we have in place to ensure our organisation remains compliant with national standards for IG? 4. "Do we as an organisation have the capacity and capability to guarantee our plans for IG can be implemented?" 5. "Do our IG arrangements adequately encompass all teams and work areas that we are legally accountable for?"
Account-able Officer	Has overall accountability and responsibility for governance within the organisation. Is to provide assurance that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
Senior Information Risk Owner (SIRO)	Has overall responsibility for ensuring that effective systems and processes are in place to address the Information Governance agenda. • Fosters a culture for protecting and using data. • Ensures information risk requirements are included in the corporate Risk and Issue Management Policy. • Ensures Information Asset Owners (IAOs) undertake risk assessments of their assets. • Is responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt. • Provides a focal point for the management, resolution and/or discussion of information risk issues. • Ensures that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff. • Ensures the Governing Body is adequately briefed on information risk issues. Is accountable for information risk. The SIRO roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance. The role holder will be supported and advised by the IG Team.
Caldicott Guardian	The role of the Caldicott Guardian is an advisory role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality & information sharing issues. The Caldicott Guardian is supported in this role by the IG Lead and IG Team who provide the Caldicott Function for the organisation.

Role	Responsibilities
Information Security Officer	This role will be fulfilled by the North East London CSU IG Team, IT team and local facilities management depending on the requirement. Provide advice to information owners on potential information risks and controls. Support in any risk reviews with departments.
Information Asset Owners	All senior staff at Director level are required to act as Information Asset Owners for the information assets within their remit. They will provide assurance to the SIRO that information risk is managed effectively for the information assists identified as within their remit. • Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed. • Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate. The IAOs will be supported by IAAs who will ensure the above takes place. The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance
Information Asset Admini-strators	Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how they work and how they are used. They will ensure there are procedures for using them, control access to them and understand their limitations. The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance
Information Governance Lead	Senior CCG Manager responsible for ensuring suitable advice, guidance support, tools and training are available to those with the CCG who handle data, to ensure they do so appropriately. This role will be the main point of contact for the NEL CSU IG Team.
NEL CSU IG Team	Provide specialist advice and support, under contract, to the organisation in relation to information governance subject matters. They will also form part of the Caldicott function.
All Substantive /Permanent Staff	All those working for the CCG have legal obligations, under the Data Protection Act and common law of confidentiality; and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct to manage information appropriately. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract.
Third parties	The same responsibilities as for permanent staff apply to those working on behalf of the organisation, whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of, but not directly employed by, the organisation are required to sign a third party agreement outlining their duties and obligations.

Role	Responsibilities
CCG Member Practices	This policy should be followed where any member is processing information on behalf of or in relation to the CCG delivery of its functions. However it is recommended that similar policy standards are in place within each member practice regarding the management of its own data and information.
Managers	**All staff with a management or supervisory role have a responsibility to ensure that all staff have been shown how to access this and related policies, supporting guidance and training.**
IT System and Service providers	System providers will provide secure, reliable IT network infrastructure with associated controls as outlined within this policy
RA Manager	Put appropriate Registration Authority (RA) systems and processes in place to enable compliance with this policy and best practice guidance.
RA Agent	The RA Agent will be responsible for ensuring RA services are delivered to users of RA services in accordance with RA policy and procedures, including registration of sponsors and healthcare professionals in the organisation
RA Sponsor	The RA Sponsor will be responsible for approving, where appropriate, the registration and profiles to be granted to users. Additionally, they may be responsible for the appropriate issue of Fallback Smartcards, Passcode resetting, vouching for the identity of users, and leaver notifications.

6. Policy Standards

This policy document, as part of a suite of supporting Information Governance related policies, sets out the standards that those working for or on behalf of the CCG are expected to adhere to when handling data or information.

6.1. Accountability and Governance

The CCG will put in place suitable controls to:

- Assign responsibilities to oversee the delivery of standards set out in this policy
- Report on compliance against Information Governance to a suitable committee within the organisation;
- Ensure that all staff have been made aware of their responsibilities, how to comply with them and have available advice and guidance and training programmes to do so;
- Ensure the consistency of information governance across the organisation;
- Develop information governance policies and procedures;
- Ensure compliance with Data Protection, and other information security related legislation;
- Provide support to the Caldicott Guardian and Senior Information Risk Owner (SIRO).

6.2. Managing Information Risk

The CCG will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and processes. A failure to effectively implement information could lead to the following risks.

Risk	Example
Reputational Damage	• Making decisions from inaccurate information could undermine any commissioning decision and could affect organisational reputation.
Financial Loss	• Loss of information could lead to financial penalties of up to £500,000 • Inefficient use of information may lead to duplication and wasted time
Failure to comply with legal, regulatory or NHS requirements	• There are a number of lawful requirements to manage information such as the Data Protection Act, Freedom of Information Act, Public Records Act which could also lead to reputation or financial loss • Failure to be compliant with NHS Constitution or NHS Care Records Guarantee or CCG Authorisation requirements.

CCG Information Asset Owners (IAOs) must ensure that information assets are assessed for risk regularly in line with Risk Management Policy and guidance. Results of risk assessments should be placed on risk registers and escalated as per the Risk Management Policy and guidance.

6.3. Information Assets & Register

Information as with any other assets of the organisation should be seen and recoded as an asset, which can take many forms. For the purpose of this policy the key assets that IAOs should be identifying are those which contain:

Manual and electronic information managed by Information Asset Administrators (IAAs) and IAOs that fall under the categories:

- Records containing personal information such as HR and Patient information and electronic systems with the data within records

Software and non-portable hardware assets will be recorded by the IT Service and people recorded by Human Resources.

Once information assets have been identified, the IAOs must log each on a local register and identify associated assets along with the risks and corresponding controls.

Where suitable controls are not in place an action plan will be agreed with the relevant IAO, IAA and IG Team on behalf of the SIRO to address any shortfalls and risks recorded on the corporate risk register.

6.4. Data/Information Classification

Information assets should be classified using the adapted NHS national classification scheme. All information assets should be classified and marked according to the following terms.

Marking	Description
NHS Official	All routine CCG business, operations and services should be treated as OFFICIAL. Ordinarily NHS Official information does not need to be marked.
NHS Official-Sensitive	This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.
NHS Official-Sensitive:Personal	Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.
NHS Official-Sensitive: Commercial	Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG, other NHS bodies or a commercial partner if improperly accessed.

The above have replaced the former markings since 1 February 2014. While the new markings do not need to be applied retrospectively, any documents and resources used from now on which contain personal or sensitive information as above will need to comply with these markings. Where practical, the relevant markings should be entered in both headers and footers, and on the front page of any reports.

NHS Official Sensitive, Commercial and Personal Information should be secured using the standards set out in this policy for as long as they are held until securely disposed of.

6.5. Information Security incident management

All staff are responsible for ensuring that any actual or potential Incidents are reported in line with the Incident Policy which includes Information Security related incidents. Such incidents include, but are not limited to:

- **Loss or potential loss of Personal Data/Information**
  - Lost Records,
  - Stolen files, diaries, Memory Sticks, Laptops, CDs etc.
  - Theft of IT equipment
- **Breach of Confidentiality**
  - Unauthorised disclosure of information e.g. release of confidential information to the wrong person, people opening the wrong mail, faxes sent to the wrong place/person, post not arriving to its intended destination
  - Leaving confidential / sensitive files out
- **Inappropriate use/access to personal information**
  - Access to data/information is not restricted
  - Personal Data/Information left unattended

- Using/sharing another user's login id and password
- Accessing a person's record inappropriately e.g. viewing records of family members, neighbours, or friend etc.,

Incident Investigation

Any incident investigation will take place in line with local guidance and national policy and serious incidents will follow root cause analysis approach.

Forensic Examination

Forensic Examination is the ability of an organisation to make use of evidence when required. Any investigation involving Information and Communications Technology (ICT) systems is likely to involve digital evidence and may therefore involve forensic examination.

Forensic Examination may be used when necessary as part of an incident investigation process. To ensure evidence is not corrupted specific procedures will be put in place to ensure the validity of electronic evidence. Please speak with the IT Team should this be required.

Internal and External Reporting of Incidents and Risk

The organisation must report those Information Security Incidents that are deemed to be an IG Serious Untoward Incident (SUI). Only minor Information Security Incidents should not be treated as an SUI.

The Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) category is determined by the context, scale and sensitivity. Every incident can be categorised asfollows:

1. Level 0 or 1 - confirmed IG SIRI but no requirement to report to ICO, DH and other central bodies/regulators.
2. Level 2 - confirmed IG SIRI that must be reported to ICO, DH and other central bodies/regulators.

The CCG will use the Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation to determine the severity of the incident.

6.6. Recruitment and Contracts of Employment

The organisation will put in place:

- Recruitment and selection processes that ensure
  - Proof of identity to e-GIF level 3 standards
  - Reliability to work within the organisation and with relevant sensitive data
- Contracts of employment which contain appropriate clauses to maintain the confidentiality, availability and integrity of data in line with this and relevant policies.

6.7. Staff Changes (Starters Leavers and Movers)

Managers will be responsible for notification of new staff or changes in role which affect access rights to any IT Systems. System managers will receive details of movement of employed staff via notification of central HR System changes, however managers retain responsibility to ensure access rights are appropriately established from effective dates.

6.8. Business Continuity

Service level plans will be in place to maintain the continuity of business should existing manual or electronic systems fail or become unavailable. This will form part of the wider organisational business continuity plans.

This will be supported by an IT Business Continuity Plan in the event of major incidents involving network and infrastructure related issues.

7. Electronic Information Security

7.1. Networks

The CCG recognises the need for a secure and reliable system to transfer electronic information securely and efficiently as a critical system to enable the delivery of business. The IT service provider will make provisions to ensure the network is secure in line with the requirements set out within this policy, supporting guidance and industry best practice.

7.2. Remote/Off Site Access to Electronic Information working

Any access to Information remotely or off site must be secure and handled as it would on site in line with this policy. The organisation, at its discretion, will provide staff with access to computer systems in line with this policy and underpinning guidance and procedures.

Any equipment provided will remain the property of the organisation and items such as Laptops, mobile phones and any other equipment provided by the organisation should only be used by the allocated member of staff for business purposes other than pre-approved personal use.

7.3. Internet & Email

Please see, the separate Calendar, Email and Internet Policy.

7.4. Use and Installation of Software

Any use of software must have been approved by the IT service provider as being suitable for use and installation. The review will include:

- Review of licensing compliance with proposed use
- Ensuring compatibility with currently installed systems
- Arrangements for support and updates
- Having a user form part of the IT Testing Group

Software installation should take place by the IT service provider following the suitable checks. Staff should note that it is a criminal offence to make/use-unauthorised copies of commercial software and offenders are liable to prosecution.

7.5. Personal Use of IT Systems

Personal use of IT systems outside of an employee's working hours is also permissible by agreement through line management. This must not involve the access of any work related NHS Sensitive, Commercial or Personal data/information.

For example, you would be allowed to access word processing facilities to update your Curriculum *Vitae*. (CV) or write a personal letter.

You must ensure that your personal use:

- Does not interfere with the performance of your duties;
- Does not take priority over your work responsibilities;
- Does not cause unwarranted expense or liability to be incurred by the organisation;
- Does not have a negative impact on the organisation in any way;
- Is lawful and complies with this policy;
- Is agreed with a line manager first
- Is during unpaid times e.g. breaks or lunches
- Not be accessed in areas that are in view of patients or members of the public.

For storage of any information generated under personal use see the Personal Electronic Information Storage section of this policy.

7.6. Use of Non-CCG Equipment to access information

Individuals (staff/contractors/suppliers) may wish to access electronic information owned by the organisation on their own personal devices, such as PCs, Laptops, Smartphones, PDAs or other electronic devices. The organisation does not expect this of staff. However, it will make arrangements to support this where appropriate.

This will be under the provision that it will take no ownership or responsibility for any issues that may arise with equipment not owned by the organisation. The arrangement must ensure the data is secure at all times. The organisation reserves the right to refuse access where controls cannot be established or would be costly to do so.

7.7. Electronic Information Storage

Information must be stored securely at all times. The specific controls will vary depending on the nature of the device. All electronic information should be stored on a networked drive with access limited to only those that require access. On some occasions it may be required that data is stored elsewhere on a short term basis. This should be risk assessed and the following controls in place as a minimum:

- Portable Media & Laptops - Each device will be encrypted to allow storage of data for a short term basis and must be transferred back to the original location as soon as is practicably possible.
- Desktop PC – no data will be stored on individual desktop PCs (C:\) without encryption storage of NHS Official Sensitive, Commercial and Personal Data. This will only be used for a short term basis and must be transferred back to the original location as soon as is practicably possible.

Data located upon network servers will be backed up in accordance with the written back-up procedures managed by the IT service provider. Such information will be stored off-site, in fire proof storage to ensure security and availability. All back-ups will be erased when no longer required.

If information is copied between systems within the network, then staff should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the first.

7.8. Personal Use of Electronic Storage

Personal drives (H:/) are for staff to store their own personal data/documents, this is not for work related storage. A limit will be placed at 250Mb after which users will be unable to store further data. The following items are not an exhaustive list but must not be stored for personal use, in any location:

- Music Files
- Video/Films Files
- Games/ Other unauthorised Software

If after investigation, such files are found they will be removed. This does not apply for authorised business related use (authorised by a line manager). However, the items will need to be stored in alternative network storage to a given personal drive (H:/). Any misuse will be deemed as breach of this policy and subject to disciplinary and/or legal action.

7.9. Use of NHS Registration Authority and Smart Cards

NHS smart cards are issued to access national systems and are authorised to enable single sign on to applications on the IT Network. All individuals with a smartcard are bound by the terms and conditions agreed prior to being provided with a card. Any misuse defined within the terms and conditions will be deemed as breach of this policy and subject to disciplinary and/or legal action.

The organisation will, through this policy, require staff to follow Registration Authority Policies and guidance developed.

Accounting & Audit

The following physical security accounting and audit logs shall be maintained:

- Physical access code changes (as agreed by SIRO/Quality Committee and immediately if needed);
- network configuration changes;
- The following audit tasks shall be performed:
- 6 monthly – audit of the accounting logs for all of the above;
- Annually – sample audit of any of the above within giving 7 days notice; and
- Annually – on a random basis, and on detection of a potential security weakness.

7.10. Encryption

All electronic data held/transferred on portable data must be encrypted to the minimum standard specified within this policy. The present standard for data being transferred across the internet or by removable media is AES256 encryption as a minimum standard. Passwords for encryption must meet those defined within the password section of this policy.

7.11. Access Controls and Passwords

All electronic information assets will have in place a process for the issue of unique access to each system. This must only provide access to only the information required to undertake ones duties, known as Position or Role Based Access Control. (PBAC/RBAC)

Access Control

The access control processes will take account of security requirements of the system and will be granted only on documented approval of an application by the relevant system manager. The process will be auditable.

Accounts must be deactivated when a user no longer requires access to the system, but remain in place in line with the records management policy for audit control purposes. Dormant Access Control accounts will be deactivated after 3 months of inactivity (non-use) and removed 12 months after this period.

Generic accounts, that do not allow unique access to systems as such will not be used as a matter of course. Any use will carry with it a risk of unsuitable controls, which the IAO (Service Manager) must document, mitigate risk and take responsibility.

No individual will be given access to a live system unless trained and made aware of his or her security responsibilities.

Passwords

Where passwords are used to restrict access to electronic information assets they must meet the following specification:

- are not names or have other connections to the user
- be a minimum of 8 characters
- are changed regularly (every 90 Days)
- cannot be the same as the last 24 passwords
- are a mixture of letters (CAPITALS and lower case), numbers and symbols
- are not shared or insecurely stored – unless in line with Legitimate Password Sharing
- users should be locked out after 3 failed logon attempts.

If a default password is used for accounts set-up by an administrator the user must be prompted to change the password. Where systems are not able to comply with the requirements see the compliance and monitoring section of the policy.

Failed password attempts will be logged and monitored by Information Asset Owners (IAOs) to identify attempts to gain unauthorised access to systems. Any identified attempts will be investigated as a breach of this policy.

Where passwords have been intentionally given to other users, the account holder will be held responsible for destructive or illegal activity carried out by an unauthorised user to whom access has been given. Unauthorised access may contravene the Computer Misuse Act (1990) and Data Protection Act (1998) and other legislation leaving *the user* open to prosecution.

Legitimate Password Sharing

When sending information from one place to another in an encrypted form, the recipient must also have the password (key) to open the relevant information, or else it will be useless. In this circumstance you should still maintain the advice for strong passwords, but can release it to the appropriate persons.

Overriding Access Controls

In justifiable circumstances access to an individual's files, folders and systems will be granted to a line manager or investigating officer. This will only be authorised by consent of user or written request from; a line manager (with HR approval), Counter Fraud Office or equivalent investigating officer. This will ensure that proper auditing of access made can be maintained and security of original user account is not compromised.

7.12. Clear Screen Policy

Computer systems will operate an automatic lock out facility when not in use to prevent unauthorised access. This period will be set to 10 minutes; however users are expected to lock access when away from the desk. (Windows Key & L).

7.13. Anti-Virus & Spyware

The CCG recognises the threat to its information assets through malicious programs and as such has put in place a system to check and remove such programs from the network and hardware. Each device must link to the network on a quarterly basis to ensure its protection is updated.

Staff must be aware of computer viruses and contact the ITServiceDesk.Anglia@nelcsu.nhs.uk if a virus incident is suspected.

7.14. Firewalls

The organisation will have in place suitable firewall(s) to prevent unauthorised network access to systems by external sources. This will be in place at all times and a process in place to authorise access accordingly, this will be managed by the IT service provider.

7.15. Portable Data Storage Devices

The CCG will monitor and at times log what documents have been saved to a device. There will also be restrictions on the use of Portable Data Storage Devices attached to PCs/Laptops or other electronic equipment to ensure any transfer to them is secure. These devices include

- USB Devices
- Memory Cards (SD/MMC etc.)
- Phones, Smartphone's, Blackberries
- CDs/DVDs/Floppy Disks/Storage Tapes

There is additional software that will:

- Allow printers, scanners, keyboards, smartcard readers and mice full access
- Allow Portable Data Storage Devices to be read on PCs and Laptops

- Prevent Portable Data Storage Devices from having data saved to them unless it is secure (encrypted). Such Portable Data Storage Devices will require authorisation to ensure:
  - The device is owned by the organisation
  - Suitable encryption will be enforced If data is to be transferred to it
  - It should only be used for work purposes

7.16. Penetration Testing

The organisation will have in place a programme of annual penetration testing to ensure IT infrastructure is appropriately secure; this will be managed by the IT service provider.

8. Physical Security Controls

It is the responsibility of all CCG staff to make their area of work as secure as is reasonably possible.

8.1. IT Server and Communications Rooms

All IT server and communications rooms must be locked at all times. All Staff working in the IT server room must be trained on the fire prevention systems in use.

All CCG staff must be accompanied at all times while conducting work in the server room by a member of the IT service provider. This can be arranged through the ITServiceDesk.Anglia@nelcsu.nhs.uk

- ICT equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality;
- Critical or sensitive ICT equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and access controls to limit access on a strict need-to basis only;
- Rooms containing ICT components such as servers providing network services, active network devices and patching for example, shall be contained in rooms that are locked at all times when not occupied;
- Critical and sensitive ICT equipment will be protected from power supply failures;
- Critical and sensitive ICT equipment will be protected by intruder alarms and fire suppression systems where available;

8.2. Clear Desk Policy

The organisation will adopt a clear desk policy, whereby any NHS Sensitive, Commercial or Personal information must be placed out of sight and access to unauthorised persons i.e. in locked cabinets or drawers when not in use.

8.3. General Physical and Environmental Security

The policy requirements are:

- All media that may store NHS Sensitive, Commercial or Personal information data should be stored in a secure, locked environment when not in use.
- Door lock codes for rooms, cabinets and cupboards containing NHS Sensitive, Commercial or Personal data should be changed regularly or following a potential or

actual compromise of the code, or when a relevant member of staff changes role or leaves.

9. Sharing of Personal Information & Transfer of data/information

The transfer of any NHS Sensitive or Personal information must:

1. Be reviewed and a lawful basis established to transfer it

2. Follow the principles and underpinning guidance to maintain the security of the information in transit.

Data Flow Mapping

Routine transfers should be logged regardless of size to allow review of security procedures in place and compliance with Information Governance requirements. IAOs are required to identify and log the routine transfers of data that will take place including

- Lawful basis
- Use of approved method
- Volume
- Frequency
- Risks
- Compensating controls

Fax Policy

The CCG will make available guidance on how to securely exchange information. However, it will specifically discourage the use of faxes to transfer information unless absolutely necessary.

10. Secure Disposal of Information

All NHS Sensitive, Commercial or Personal information must be securely disposed of using the relevant guidance documents.

10.1. Disposal of Manual Information

Manual information will be disposed of using certified confidential shredding services to BS 8470 standards. Details of destroyed information and certificates should be held in accordance with the Records Management Policy. A certificate of destruction of the data and, where appropriate, devices are to be kept for the relevant retention period.

10.2. Disposal of Electronic Storage Media Information

Electronic assets - CDs, Memory Sticks, Hard Drives, Laptops, Desktop PCs, and Personal Data Assistant (PDA) etc. must be disposed of securely using a certified disposal provider, arranged by the ITServiceDesk.Anglia@nelcsu.nhs.uk

11. Relationship with Service Providers

As a commissioner of clinical and support services the CCG will ensure that any organisations from which it buys services meets expected information governance standards.

11.1. Clinical Services

All clinical services commissioned by or on behalf of the CCG will be required to:

- Have a suitable contract (or if more appropriate, Service Level Agreement - SLA) in place to form a joint data controller relationship in relation to the information required to effectively monitor commissioned services.
- Ensure the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office.
- Completion of the annual Information Governance Toolkit and undertake an independent audit to be disclosed to the CCG on request to provide assurance they have met expected requirements.
- Ensure privacy notices make individuals aware of a CCGs role in commissioning and the personal and sensitive data it may receive to undertake such a role.
- Ensure that where any IG incidents occur that they are reported to the CCG via routes determined within the contract.
- Ensure the contract stipulates sufficient security controls to meet or exceed requirements set out in this policy.

11.2. Support services

All support services that process information on behalf of the CCG will be required to ensure:

- The contract (or if more appropriate, Service Level Agreement - SLA) stipulates sufficient security controls to meet or exceed requirements set out in this policy.
- Suitable contract is in place to form a Data Controller to Data Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG
- The services commissioned meet the requirements of the Data Protection Act when providing services including but not limited to fair processing, maintaining a registration with the Information Commissioners Office
- Completion of the annual Information Governance Toolkit and undertake an independent audit to be disclosed to the CCG on request to provide assurance they have met expected requirements.
- That any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity
- Report any known incidents or risks in relation to the use or management of information owned by the CCG

12. Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with expected Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as “minimal impact”.

13. Training requirements

Information Security is fundamental in everyone's training, and therefore will form part of mandatory training. This will be reviewed and documented within the IG training needs analysis and delivery plan, to ensure it meets the relevant job roles within this policy.

14. Dissemination and Implementation

This policy will be made available to all relevant stakeholders via the CCG internet site. Additionally they will be made aware via email and this policy will be included for reference where necessary.

The policy will be supported by additional related policies and resources to support implementation. This will include the availability of, and access to, written and verbal advice, guidance and procedures where necessary.

15. Non-Conformance with this Policy

Should it not possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the department's Information Asset Owner. Any issues will need to be documented as a risk and either:

a. Accepted and reviewed in line with this policy
b. Accepted with a view to implementing an action plan to reduce the risk
c. Not accepted and the practice will stop until such time as the risk can be reduced

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958

16. Monitoring and Review

Performance against the policy will be monitored against

- Availability and dissemination of policy and in alternative formats where requested or need identified
- Acceptance and understanding of audience (training, spot checks, surveys)
- Reports of non-conformance i.e. incidents or risks
- Compliance against the Information Governance Toolkit.

This policy will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:

- Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risks or following significant incidents reported;
- Changes to organisational infrastructure.

16.1. Monitoring of individuals

In order to ensure compliance with the Law and organisational policies (including this one), the CCG reserves the right to monitor usage and content where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

In addition, communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of the CCG's business, and the employee's position with the CCG. Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

This will include the use or access to any Network or where the property of the Organisation is used in the communication or is accessed remotely from outside the Organisation. This includes the use of portable computers and mobile devices, including mobile phones issued to the employee by the Organisation.

Appendices

Appendix A. Evaluation protocol

Monitoring requirements 'What in this document do we have to monitor'	The management of information risks (Information Risk Management) Compliance with the law Compliance with the Information Governance Toolkit Incidents related to the breach of this policy Destruction of Information Assets Registration of Data Flows and Information Assets Compliance with Registration Authority Terms and Conditions Network Penetration testing Monitoring of inappropriate access to systems (where possible)
Monitoring Method	Information Risks will be monitored through the Risk Register and management system. Compliance with law will be monitored through audit, work directed by the Information Governance Toolkit and as directed by the SIRO The Information Governance Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the IGT will be audited by the organisation's internal audit function before the annual submission. Incident reporting and management requirements
Monitoring prepared by	The CSU Information Governance Team and the CCG IG Lead for the relevant groups Incident reports will be produced by the nominated investigation officer
Monitoring presented to	Relevant CCG committees or groups with oversight of Information Governance Senior Information Risk Owner Caldicott Guardian
Frequency of Review	Yearly updates will be provided to the relevant groups, the SIRO and the CG Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system Annual (as a minimum) updates to the Board will be provided. The internal audit report on IGT performance will be provided to the Board or delegated sub-committee. Incident Reports will be reviewed on an annual basis and as directed by the seriousness of the incident

Appendix B. Equality Analysis

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

	Challenge questions	**Yes/ No**	**What positive or negative impact do you assess there may be?**
1.	Does the proposal affect one group more or less favourably than another on the basis of:	No	
	▪ Race	No	
	▪ Ethnic origin (including gypsies and travellers, refugees & asylum seekers)	No	
	▪ Nationality	No	
	▪ Gender	No	
	▪ Culture	No	
	▪ Religion or belief	No	
	▪ Sexual orientation (including lesbian, gay bisexual and transgender people)	No	
	▪ Age	No	
	▪ Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)	No	
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)	No	
3.	Will the proposal have an impact on social environment? (e.g. social status, employment (whether paid or not), social/family support, stress, income)	No	
4.	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)	No	
5.	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)	No	

Appendix C. Information Assets

This is an illustrative list of the types of information Assets an organisation may hold based upon Connecting for Health guidance

Personal/Other Information (to include Manuel and Electronic)

- Paper Records and Reports (e.g. Patient/Staff Records, Clinical/Corporate)
- Databases
- System Documentation
- Process documentation
- Back up and Archive Data
- Audit Data
- Patient case notes and staff records
- Paper reports

Software

- Application Programs (e.g. Microsoft Office)
- System Software (e.g. Windows package)
- Data Encryption Utilities
- Development and Maintenance Tools

Hardware

- Computing Hardware including PC's, Printers etc
- Laptop
- Blackberry
- Removable Media (Pen sticks, External Hard Drives, CD's, Other)
- Mobiles
- Computing & Networks infrastructure and Connections

People

- Qualifications
- Experience
- Skills
- PDR's
- Employment Position/Job Description
- Leave records

Physical

- Equipment (Clinical and Non-Clinical)
- Furniture
- Infrastructure
- Buildings

Services

- Lighting
- Heating
- Air-Conditioning
- Lifts
- Communications (e.g. telephone)
- Power

Appendix D. Information Security Policy Summary Sheet

Information Security Policy Summary Sheet

This checklist is intended to be a helpful Information Security aide-memoir for Staff. It is not intended to be a comprehensive summary of user responsibilities and does not reduce or alter the standards or principles in the Information Security Policy.

All Staff should:

- Understand what information they use is:
  - NHS Sensitive
  - NHS Personal
  - NHS Commercial
- Speak with your line manager if you are aware that you are not meeting the standards and principles of the Information Security Policy
- Be aware of the potential risks that surround the data/information you use.
- Store all sensitive information on central file servers (L:/,K:/) and not on personal computers or drives (C:/).
- Safeguard portable IT equipment. Do not leave them visible and unprotected in public places.
- Portable hardware must be installed with encryption
- Follow password protection guidance
- Dispose of any confidential electronic or manual data/information securely
- Log off or lock computers if you are not using them (Windows Key + L)
- Wear your staff identification badge at all times
- Report incidents using the appropriate mechanisms

Staff should not:

- Move any non-portable IT equipment without contacting the Helpdesk
- E-mail NHS Confidential or NHS Protect information without following the Internet & Email Policy
- Share passwords or use someone else's password
- Copy personal data from one system to another without confirming that the recipient system has the same or greater security protection
- Use or try to use IT networks which you have not been authorised to use
- Copy software without the authority of the copyright holder.
- Store confidential information on portable IT equipment such as Laptops and Pen drives without encryption being used

Appendix E. Definitions used in this policy

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)* based on the Cabinet Office definition
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)