NHS
North Lincolnshire
Clinical Commissioning Group

Information Security Policy

Authorship:	Information Governance
Committee Approved:	Integrated Audit & Governance Committee
Approved date:	03/03/2021
Review Date:	2 years from approval
Equality Impact Assessment **Sustainability Impact Assessment** **Data Protection Impact Assessment** **Target Audience:**	**Screening** **Completed** **Not Required** **All Staff**
Policy Reference No:	N/A
Version Number:	2.0

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.2	Chris Wallace	First draft for comments		
1.0	Barry Jackson	Approved version		
1.1	Mark Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).		
2.0	Hayley Gillingwater	Updated Bribery Act GDPR Addition of NLincs Council's (IT Provider's) security standards. Incidents Data Security & Protection Toolkit Removal of eMBED Back up procedures	IACG 03.03.21	

Contents

1 INTRODUCTION AND APPLICABILITY

Information and information systems are important assets to every organisation and it is essential to take all the necessary steps to ensure that they are comprehensively protected, available and accurate to support the operation and continued success of the CCG at all times.

The Information Security Policy is a key component of the CCGs overall information security management framework and is designed to:

- provide a corporate framework in which security threats to our Information Systems can be identified and managed;
- illustrate the CCGs commitment to the security information and information systems;
- provide accepted formal procedures to ensure a uniform implementation of security measures;
- introduce and formalise procedures to minimise the risk of unauthorized modification, destruction or disclosure of information; and
- align the organisation to the NHS Information Governance aims and expectations described in the Information Security Management: Code of Practice for NHS Organisations.

Note: these objectives can only be achieved if every staff member observes the highest standards of personal, ethical and professional conduct in relation to the handling and management of information.

1.1 Requirement for Security Policy.

The CCG acknowledges that information is a valuable asset, therefore it is within its interest to ensure that the information it holds is suitably protected from any threat. By protecting its information the CCG is acting in the best interests of its employees and all third parties with whom information is shared whilst minimising key risks associated with information processing:

- loss of public confidence in the CCG
- contribution to clinical or corporate negligence
- loss of equipment

Key issues addressed by the Security Policy are:-

- Availability - information is delivered to the right person when it is needed.

- Confidentiality - data access is confined to those with specified authority to view the data;
- Integrity - all system assets are operating correctly according to specification and in the way the current user believes them to be operating; and

The CCG intends to achieve a standard of excellence in Information Governance by ensuring all information is dealt with legally, securely, efficiently and effectively in order to support the delivery of high quality patient care, service planning and operational management. For this to be achieved information processing must comply with legislation and best practice and the CCG will establish and implement policies and procedures to ensure appropriate standards are defined, implemented and maintained.

1.2 Legal Compliance

The CCG is bound by the provisions of a number of items of legislation affecting the stewardship and control of patient and other information. The main relevant legislation is:

- The Data Protection Act 2018The General Data Protection Regulation (GDPR)
- Access to Health Records Act, 1990 (where not superseded by the Data Protection Act, 1998);
- Computer Misuse Act, 1990;
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998; and
- The Human Rights Act 1998.

This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected. In addition to the above, other legislation can impact upon the way in which we should use personal information. This includes:

- Public Interest Disclosure Act 1998;
- Audit & Internal Control Act 1987;
- Public Health (Code of Practice) Act 1984;
- NHS (VD) Regulations 1974;
- National Health Service Act 1977;
- Human Fertilisation & Embryology Act 1990;
- Abortion Regulations 1991;
- The Terrorism Act 2000;
- Road Traffic Act 1988;

- Regulations under Health & Safety at Work Act 1974.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.
- Health and Social Care Act 2012
- Health and Social Care Act (Safety and Quality) 2015
- Records Management Code of Practice for Health and Social Care 2016

Much of the legislation mentioned is available in electronic format, via the Internet (www.legislation.hmso.gov.uk). In addition, the CCG is bound by the confidentiality aspects of common law and the Caldicott guidance on protection of patient information.

As part of, and in addition to, the above legislation the CCG is required to retain all records (health and administrative) for specified periods of time. For further information on this see the Records Management Policy and NHS England's Corporate Records Retention Schedule.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

3.3 General Data Protection Regulation (GDPR)

The CCG is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the CCGs Data Protection and Confidentiality and related policies and procedures. If you are commissioning a project or undertaking work that requires the processing of personal data you must complete a Data Protection Impact Assessment. Please see the CCG's Data Protection Impact Assessment Procedure and Data Protection by Design & Default procedure available on the website for guidance.

3.4 Bribery Act 2010

The Bribery Act is particularly relevant to this policy. The CCG has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010. Under the Bribery Act 2010 there are four criminal offences:

- Bribing or offering to bribe another person (Section 1)
- Requesting, agreeing to receive or accepting a bribe (Section 2);
- Bribing, or offering to bribe, a foreign public official (Section 6);
- Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both. They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by the CCG, whether or not the breach leads to prosecution. Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

It is the duty of every member of staff to speak up about any genuine concerns in relation to criminal activity, breach of a legal obligation, miscarriage of justice, danger to health and safety or the environment and the suspected cover up of any of these in the workplace. To raise any suspicions of bribery and/or corruption please contact the Chief Finance Officer. Staff may also contact the Local Counter Fraud Specialist on 07872 988939/

email nikki.cooper1@nhs.net or Head of Anti-Crime Services on 07717 356707 / email steven.moss@nhs.net.

The LCFS or Chief Finance Officer should be the contact for any suspicions of fraud. The LCFS will inform the Chief Finance Officer if the suspicion seems well founded and will conduct a thorough investigation. Concerns may also be discussed with the Chief Finance Officer or the Audit & Integrated Governance Committee Chair.

If staff prefer, they may call the NHS Fraud & Corruption Reporting Line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at www.reportnhsfraud.nhs.uk. This would be the suggested contact if there is a concern that the LCFS or the Chief Finance Officer themselves may be implicated in suspected fraud, bribery or corruption.

4 SCOPE

The Information Security Policy applies to all business functions within the CCG and all third-party services that provide a service on behalf of the CCG. The policy covers data, information systems, networks, physical environment and relevant people who support these functions. It relates to both manual and electronic information, whether transmitted across the N3/HSCN network, personal email addresses, Skype, Microsoft Teams, or telephone lines, spoken in conversations or printed as hard copy.

5 POLICY PURPOSE & AIMS

Operating Procedures and Standards

5.1 Compliance

It is the policy of the CCG to ensure compliance, in accordance with all the legislative obligations. The CCG also requires all employees, contractors and third parties to comply with this policy and supporting standards and procedures where appropriate.

5.2 Information Security Awareness and Education

It is the responsibility of all employee’s and third parties of the CCG to sustain excellent information security. To comply with this, the CCG requires all employees and contractors within scope to understand the importance of information security and be familiar with this document and supporting documents where appropriate.

To facilitate this information governance training will be included in the staff induction process and as an annual requirement in order to ensure staff awareness is refreshed and updated as necessary. This is a mandatory requirement; failure to complete data security and awareness training may result in disciplinary procedures.

5.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. In addition, information security expectations of staff shall be included within appropriate job definitions.

5.4 Email and Electronic Systems

The CCG has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The procedures cover use of any systems used to store, retrieve, manipulate and communicate information (e.g., telephone, e-mail, Skype, Microsoft Teams, IT systems and the Internet). All employees and third parties are required to familiarise and adhere to them.

5.5 Access Controls

Physical Security:

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

In addition, each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

In order to minimise loss of, or damage to, assets equipment will be physically protected from threats and environmental hazards.

All staff are responsible for the physical security of assets and equipment used by them on behalf of the CCG. Appropriate physical security measures shall be put in place to secure information assets, dependant on value and sensitivity to the organisation.

All staff are responsible for ensuring that their work areas are left in a secure state when vacant.

User Access Controls:

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Computer Access Controls:

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities. All employees, contractors and third-party users that no longer need access to the CCG's information and information processing facilities will return all CCG assets e.g., laptops and building access controls such as electronic key fobs when requested. It is the line manager's responsibility to ensure all assets are returned.

Application Access Control:

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g., systems or database administrators.

The CCG has a procedure outlining the control of access to its premises, physical assets and electronic networks. Procedures also cover correct use of its assets. All employees and third parties are required to acquaint themselves with these standards.

5.6 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IT Department.

5.6.1 Through connection to the CCG's network it is possible to receive and forward information to other users of the network and other organisations' networks using, for example, electronic mail. Should employees receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to the IT Service Desk and the Information Governance Delivery Manager.

5.6.2 Equipment must not be used until identified by IT support staff that the system is ready for use.
All equipment used to support the storage and processing of information shall be adequately maintained according to manufacturers' maintenance schedules. All IT equipment maintenance shall be formally authorised and managed by IT Services. Computer and network equipment shall be covered by warranties or third-party maintenance agreements. Wherever possible, new equipment shall be purchased with a three years' warranty agreement. Only authorised personnel shall carry out repairs and service equipment. Documented records of all equipment faults and maintenance shall be maintained. An equipment development/refresh strategy will be maintained along with a documented log of the risks associated with non-replacement of devices.

5.6.4 Fault logging procedures and controls shall be used to address faults in information processing systems, with the ability to record fault details, the fault 'reporter', dates and times, on-going fault status and corrective actions, and to assist with the analysis of fault types, frequencies, impacts and costs. IT Services shall be responsible for implementing the fault logging procedures and controls, and regularly reviewing faults to ensure that all faults have been satisfactorily resolved, and to identify ways of improvement. All users shall comply with requirements for reporting faults to IT Services as soon as possible

5.6.5 A security log of access to the organisations network must be maintained.

5.6.4 All computer files transferred from other networks must be checked for viruses before use within the organisation.

5.6.5 Network Controls shall be implemented to achieve and maintain security e.g., firewalls, routers and switches, authentication and access controls, encryption, and logging and monitoring of access. Special controls shall be established to safeguard the confidentiality and integrity of data passing over public or wireless networks e.g., use of authentication and encryption. IT Services shall be responsible for network security.

5.6.6 All access to information and information processing facilities shall be restricted on a 'need-to-know' basis. As far as possible, each user shall access information using a unique user ID and password. This policy shall be enforced by Information System/Asset Owners and IT Services.

5.6.7 Access privileges shall be limited to a level that ensures that each user is able to perform their job function (but no further functions). They shall be implemented via the procedures detailed in the User Registration process.

5.6.8 Operating system access control applies to all computers that have an operating system e.g., servers, PCs, and laptops. IT Services shall ensure that log-on procedures are secure and do not provide unnecessary information that could enable unauthorised access e.g., provide clues about valid user IDs or the operating system version (and therefore its vulnerabilities). Operating system and network domain log-on procedures shall also include an enforced user acknowledgement to comply with the Computer Misuse Act, 1990. All successful and unsuccessful log-on attempts shall be logged and monitored.

5.6.9 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. The IT provider shall implement standards and procedures for audit logging of network access, operating system access, and applications and information access, and shall identify events and details that need to be captured in audit logs. Information System Owners shall be responsible for audit logging requirements for business information systems (applications), whilst IT Services shall be responsible for audit logging requirements for the IT network and security infrastructure, user network domains, server and client operating systems, and corporate systems such as e-mail and Internet access. Responsibilities include identifying and implementing audit log retention and archiving needs to comply with legal, regulatory, contractual and evidence gathering requirements.

5.6.10 Procedures for monitoring use of information processing facilities shall be established, and the results of the monitoring activities reviewed regularly. The CCG and their IT provider, within its legal rights, shall monitor day-to-day access and use of its information processing facilities to ensure adequate protection from security threats, and where necessary, shall collect evidence of misuse and unauthorised activities. Information System Owners shall be responsible for monitoring access of business information systems (applications), whilst IT Services shall be responsible for monitoring access of the network and security infrastructure, user network domains, server and client operating systems, and corporate systems such as e-mail and Internet access. Suitable technology and adequate staff resources shall be identified and implemented to support this policy.

5.6.11 Logging facilities and log information shall be protected against tampering and unauthorised access using appropriate controls e.g., authentication and access controls. Information System Owners and IT Services shall ensure that access to log information is restricted on a ‘need-to-know’ basis, and only to ‘trusted’ staff.

5.6.12 System and database administrator activities shall be logged. This shall be the responsibility of Information System Owners and IT Services. Where necessary, logs of administrator activity shall be immediately copied to a secure area to protect against any tampering of evidence of access.

5.6.13 IT Services shall be responsible for all cryptography controls (encryption and digital signatures) used for the storage and transmission of sensitive information.

5.6.14 Software shall only become operational on the authorisation of IT Services. Only IT Services shall install or update operational software and applications, using configuration management processes. IT Services shall ensure that all computer systems, e.g., servers, PCs and laptops are 'locked down' so that no unauthorised software can be installed.

5.6.15 All employees must inform the IT Service Desk if a virus is detected or suspected.

5.6.16 Failure to immediately notify the CCG of a suspected virus or data breach may result in disciplinary procedures.

5.7 Information Risk Assessment and Asset Management

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the Information Asset Register and action plans shall be put in place to effectively manage identified risks. The Information Asset Register and all associated action plans shall be compiled and reviewed regularly by Information Asset Owners (IAOs). Any implemented information security arrangements shall also be a regularly reviewed feature of the CCGs risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed. IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review. The IAR is sent to IAOs to be updated on a bi-annual basis, IAOs are required to respond to the call for updates even if there are no changes to their assets.

5.8 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported via the CCGs Incident Management process to the Head of IT.

All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

Information Governance breaches must be reported at the earliest opportunity in order that they can be investigated in a timely manner and reported to the Information Commissioner's Office (ICO) within 72 hours if required.

Staff will NOT be subject to disciplinary proceedings for basic human errors or genuine mistakes. However, failure to report known breaches will be taken seriously.

5.9 Classification of Sensitive Information

The CCG will implement information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security & Protection Toolkit to secure their NHS information assets. Further guidance on information classification is contained within the CCG Records Management Standard and Procedures.

5.10 Protection from Malicious Software

The CCG will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users will not install software on the CCGs property without permission from the Associate Director of IT. Users breaching this requirement may be subject to disciplinary action.

5.10.1 Under the Computer Misuse Act 1990 'hacking' and the introduction of computer viruses are criminal offences. The purpose of the Act is to make provision for securing computer material against unauthorised access or modification. It makes unauthorised access to a computer, programs or data an offence.

5.10.2 Staff should report any viruses, suspected viruses or suspicious emails (which could contain viruses) to the IT Service Desk.

5.10.3 All information management and technology security (Cyber) incidents and weaknesses must be reported immediately in line with the CCG Incident Reporting Policy.

5.10.4 Information Security Incidents, especially those involving the loss of sensitive or confidential data, or any incident involving unencrypted portable devices may need to be reported as a Serious Incident and/ or to the Information Commissioner via the Data Security and Protection Toolkit reporting system. See the Incident Reporting policy for more details.

There is a legal requirement to report any such serious incidents to the authorities within 72 hours.

All staff undertake appropriate annual data security training, renamed "Data Security Awareness Level 1" to reflect Data Security Standard 3 in the Caldicott 3 Review, and pass a mandatory test.

The CCG obtains regular assurance from the IT provider that CareCert Alerts are being acted upon and are being addressed appropriately. CareCert informs organisations about cyber security vulnerabilities, mitigating risks, and reacting to cyber security threats and attacks.

5.11 User Media

The CCG will use port control software to control the use of removable media. Access to USB mass storage devices and CD/DVD writers will be restricted to approved users only.

Where removable media is received from external sources or has been used on computers systems not owned by the CCG users are required to scan the media using anti-virus software before its use.

All removable magnetic media must be encrypted. Failure to do this may result in disciplinary action.

5.12 Accreditation of Information Systems

The CCG shall ensure that all new information systems, applications and networks include a security policy and are approved by the Associate Director of IT before implementation.

System specific security policies will be developed for systems under CCG control in order to allow granularity in the security management considerations and requirements of each. This may result in specific responsibilities being assigned and obligations communicated directly to those who use the system.

5.13 The CCG shall ensure that all new information systems, applications and networks include a Data Protection Impact Assessment (DPIA) and System Level Security Policy (SLSP) and are approved by the Information Governance Group and/or IT before they commence operation.

5.14 When planning for, and during procurement of, new systems, it is the responsibility of the Project Manager or Lead to ensure that appropriate system security features are included within the system. As a minimum this will include a password protection feature and audit logs.

5.15 Systems and applications must be adequate for their purpose.

5.16 Software applications, upgrades and amendments must be developed in a controlled manner, documented and thoroughly tested before implementation.

5.17 Proof of ownership of software licenses must be maintained and master disks held in a secure environment in the event of necessary re-install.

5.18 Unauthorised software must not be introduced onto any system without prior authorisation from the IT Service Desk/Associate Director of IT.

5.19 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Associate Director of IT or authorised officer.

5.20 Intellectual Property Rights

The CCG shall ensure that all information products are properly licensed and approved by the Associate Director of IT or suitable deputy.

Users shall not install software on the organisation's property without permission from the Associate Director of IT. Users breaching this requirement may be subject to disciplinary action.

5.21 Business Continuity and Disaster Recovery Plans

The CCG shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

It is the responsibility of all employees and contractors to familiarise themselves, as appropriate, with the business continuity plan that supports this policy.

5.22 Reporting

The Associate Director of IT or suitable deputy will keep the Executive Management Group informed of the information security status of the organisation by means of regular reports and presentations.

5.23 Policy Audit

This policy will be subject to regular independent audit and annual assessment in line with the completion of the Data Security & Protection Toolkit by internal and external audit.

5.24 Physical Security

All staff are responsible for the physical security of assets, equipment and building used by the CCG. Appropriate physical security measures shall be put in place to secure information assets dependant on value and sensitivity to the organisation.

All staff are responsible for ensuring that buildings are left is a secure state when vacant.

5.25 Policy Violations

It is a condition of employment with the CCG that compliance should be maintained where appropriate with the information security management policy and supporting standards and procedures.

If any procedures or policies are violated these will be treated as security incidents and reported in accordance with the CCGs incident reporting procedure. Failure to comply with this policy, or supporting procedures, could result in disciplinary action.

6 ROLES / RESPONSIBILITIES / DUTIES

Information Security Responsibilities

Policy review and maintenance	Chief Finance Officer / SIRO
Approval	CCG Executive Management Team
Adoption	All manager, staff and contractors

Responsibility for Information Security will reside with the CCG Executive Management Team. On a day-to-day basis the Associate Director of IT will be responsible for implementing, managing, monitoring, documenting and communicating the security requirements for the organisation.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- the information security policies and procedures applicable in their work areas;
- their personal responsibilities for information security; and
- how to access advice on information security matters

All staff will comply with information security policies and procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Line managers will be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff will be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

As part of its responsibility as a service provider the IT provider, is responsible for ensuring that network computer equipment will be housed in a controlled and secure environment and protected with a combination of technical and non-technical measures. The IT department is responsible for ensuring that network backup procedures are documented and undertaken and that business continuity and disaster recovery plans are produced for the network. The IT department will provide the CCG with regular assurance that the services supplied to the CCG comply fully with the Information Security related requirements of the Data Security & Protection Toolkit.
Regular recovery tests using back-ups shall be performed by IT Services to ensure that a 'business as usual' status can be resumed as quickly as possible following a security incident occurrence. Information System Owners shall be responsible for identifying business requirements for back-up and recovery controls (including legal, regulatory and contractual requirements for data retention), whilst IT Services shall be responsible for implementing suitable back-up and recovery controls and procedures. The successful completion of all back-ups shall be confirmed as soon as possible. Storage of back-ups shall be geographically separate from the backed-up information systems to protect against building loss.

7 IMPLEMENTATION

The policy will be disseminated by being made available on the website and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

8 MONITORING COMPLIANCE

8.1 It is the responsibility of all staff to ensure that the potential for security breaches does not occur as a result of their actions.

8.2 All staff must report instances of security breaches, near misses or weaknesses through the incident reporting procedures.

8.3 The Information Governance department will report information security incidences to the SIRO and Caldicott Guardian.

8.4 Risk Management, Information Governance and the IT department will investigate all suspected/actual security breaches and report to the appropriate bodies.

8.5 The CCG will be responsible for collating and reporting the number of breaches and ensuring actions have been taken.

8.6 The IT provider will, in conjunction with departments, provide advice and guidance on how to maintain security and confidentiality compliance across organisations.

Refer to the organisation's Incident Reporting Policy for further details.

9 TRAINING & AWARENESS

It is the responsibility of the CCG to ensure that mandatory training and induction programs are implemented to ensure the awareness of all staff with regard to Security and Confidentiality. Staff will be made aware of the policy via the CCG's website.

10 MONITORING & AUDIT

Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The CCG has in place routines to regularly audit compliance with this and other policies. In addition, the CCG reserves the right monitor activity 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

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

11 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

12 REFERENCES

Supporting Documents and Procedures

The following documents are in support of the Information Security Policy:-

Confidentiality Policy

Network Security Policy

Records Management Policy

Monitoring Standards and Procedures

Data Protection Impact Assessment Procedure

Data Protection by Design & Default Process

Information Asset Owner’s Handbook

Appendix 1 – Integrated Impact Assessment

INTEGRATED IMPACT ASSESSMENT

Policy/project/function/service	Information Security Policy	
Date of analysis:	05/02/2021	
Type of analysis completed	Quality	X
	Equality	X
	Sustainability	X
What are the aims and intended effects of this policy/project or function?	This standard documents the CCGs information security framework and security standards that are in place.	
Please list any other policies that are related to or referred to as part of this analysis	Confidentiality Policy Network Security Policy Records Management Policy Monitoring Standards and Procedures Data Protection Impact Assessment Procedure Data Protection b Design & Default Process Information Asset Owner's Handbook	
Who does the policy, project, function or service affect?	Employees	X
	Service users	
	Members of the public	
	Other (please list)	

QUALITY IMPACT

	Please 'X' ONE for each			Brief description of potential impact	Mitigation strategy and monitoring arrangements	Risk 5 x 5 risk matrix)	
	Chance of Impact on Indicator						
	Positive Impact	No Impact	Negative Impact			Likelihood	Consequence
	X	X	X				
PATIENT SAFTEY							
Patient safety /adverse events		x					
Mortality position		x					
Infection control MRSA/CDIFF		x					
CQC status		x					

NHSLA / CNST		x					
Mandatory/statutory training		x					
Workforce (vacancy turnover absence)		x					
Safe environment	X						
Standard & suitability of equipment		x					
CLINICAL EFFECTIVENESS							
NICE Guidance and National Quality Standards, eg VTE, Stroke, Dementia		x					
Patient related outcome measures		x					
External accreditation e.g. professional bodies ie RCN		x					
CQUIN achievement		x					
PATIENT EXPERIENCE							
Will there be an impact on patient experience if so how		x					
Will it impact on carers if so how		x					

INEQUALITIES OF CARE							
Will it create / reduce variation in care provision?		x					
STAFF EXPERIENCE							
What is the impact on workforce capability care and skills?		x					
Will there be a change in working practice, if so, how?		x					
Will there be an impact on training	x			Additional training may be required to ensure all staff understand the policy and their requirement to align with it.			
TARGETS / PERFORMANCE							
Will it have an impact on performance, if so, how?		x					
Could it impact on the achievment of local, regional, national targets, if so, how?		x					

QUALITY IMPACT

Analysis Rating (see completion notes)	Red		Red/Amber		Amber		Green	X
Approved by:	Commissioner Lead:				GP lead for E&D:			
	Date				Date			

Local Profile Data

General	North Lincolnshire is predominantly a rural area and neighbours; North East Lincolnshire, West Lindsey, South Yorkshire, Nottinghamshire and the East Riding of Yorkshire. North Lincolnshire is geographically large, although the population is small in comparison with some neighbouring unitary authorities. The latest midyear population estimates for North Lincolnshire estimate that 172,292 people live in the local area (ONS, 2019). This represents more than a 3.5% growth in the resident population since 2010 and an annual growth of about 640 more residents a year. The GP registered population as at April 2020 is 181,658. Nearly half of North Lincolnshire's residents, 48%, live in rural market towns and villages, where much of the recent growth in its older population has occurred. North Lincolnshire is serviced by a medium sized Foundation Trust, NLaG, which operates from 3 sites, Grimsby, Scunthorpe and Goole. Scunthorpe General Hospital services the majority of the population providing a seven day scanning/diagnostic service and a busy emergency centre with around 60,000 attendances every year.
Gender	North Lincolnshire has 50.6% female and 49.4% male population (North Lincolnshire Strategic Needs Assessment 2018, Fingertips Public Health Data).
Race	92.3% of the resident population of North Lincolnshire are "White British" and a further 3.2% are of other White origin (not including Irish and Gypsy Travellers). The proportion of ethnic minorities in North Lincolnshire (4.5%) is significantly lower than that seen in the Yorkshire and Humber region (14.2%) and in England as a whole (20.2%) The area has a relatively small Black and Black African population making up less than 1% of residents More than 53% of the BME communities live in the northern part of Scunthorpe. The largest concentration of BME children is in Scunthorpe North, where they represent more than a fifth of the primary school age population. In North Lincolnshire, unemployment amongst the BME community is more than twice that for the White UK population – 14.5% compared with 5.9% (Annual Population Census, 2012). In 2011, more than 8.1% of all school aged children were from Black and Asian communities, with at least half as many more BME children in reception classes as in Year 11. Adding 'other, (Non UK) White', to the BME total, (including White European) the proportion increases to more than 12%. 95.5% of households all residents had English as their main language, compared to 93.4% in Yorkshire and the Humber and 90.9% nationally. More than 60 identifiable different languages are spoken across North Lincolnshire, the most common being Polish, Lithuanian, Bengali and Portuguese. Based on the latest ONS (2018) predictions, net migration in North Lincolnshire is thought to have been around 590 in 2010 and 712 in 2019. Net migration within

	North Lincolnshire was expected to increase gradually, averaging around 750 people per year over the next 24 years but may be affected substantially by the UK exit from Europe.
Disability	In the last census (2011) 19% of residents identified as having day to day activities being limited either a little or lot (due to impairment or health condition); with approximately 6% of residents being blue badge holders. The Life Opportunities Survey (2011), identified that nearly one third of adults aged 16 and over had at least one impairment and 26% of adults aged 16 and over in Great Britain would be covered by the rights under the provision of the Equality Act. • 23.8% of the working population are EA core or registered as having a work-limiting disability (24,700). This is significantly higher than Yorkshire and the Humber (21.4%) and England (19.4%). • 26.7% of all households in North Lincolnshire have at least one person with a long-term health problem or disability (18,899). • 9.2% of the resident population (an estimated 15,333 residents) stated that their daily activities were significantly limited due to a health condition or disability. • 19.3% of the population had some form of day-today activity limiting disability, compared with 18.9% and 17.6% for Yorkshire and Humber and England respectively. • More women have a disability (24.7%) than men (23.0%). This is broadly significantly higher than national values and higher than Yorkshire and Humber comparator groups. • Figures for August 2017 show 5910 people claiming ESA or IB equivalent equates to 3.46% of the total population, which is lower than Yorkshire and Humber figures (3.65%), and higher than the national rate (3.22%). • In 2017, 3485 (14.3%) of school pupils were identified as having Special Education Needs - this was below the national average (14.4) and higher than Yorkshire and Humber (14.0%). Of the 3485 children receiving SEN support 755 had EHC or SEN plans.6 • According to the Census 2011, the number of residents of North Lincolnshire who stated that their 'Day-to-Day Activities were Limited a Lot' was 14,207, 8.6% of all household residents. This compares to 8.7% regionally and 7.9% nationally. However there is significant difference across the age bands, the older people become the higher the percentage of residents whose activities are limited.
Religion or Belief	• The 2011 census stated that 69% of North Lincolnshire residents identified as having a belief. 66% Christian, 2.6% Muslim and 1.8% other (Sikh, Hindu, Buddhist, Jewish or other). For Christianity, this is higher than the national average but lower for other religions. • 7.1.% of residents do not state their religion and 24% state they are of no religion
Sexual Orientation	There are limited accurate statistics available regarding the profile of the lesbian, gay, bisexual and transgender (LGBT) population in North Lincolnshire, the region, or indeed, across England as a whole. Sexuality as a whole has historically not been included in censes or most other official statistics. However, this continues to change and become integrated within demographic studies. The 2011 census estimated 185 persons in a registered same-sex civil partnership. In the Yorkshire and Humber region 94.4% of survey respondents aged 16 or over identified themselves as heterosexual/ straight. Percentages of people identifying as sexualities other than heterosexual/ straight are broadly similar for the Yorkshire and Humber and all England geographical regions with gay/lesbian being the highest percentage at 1%

Pregnancy and Maternity	Locally, according to the ONS in 2018 there were 1,673 live births registered within North Lincolnshire with 2 registered still births. On a National level, there were 657,076 live births recorded in 2018 compared with 679,106 in 2017. In 2018 339,267 of births were registered born within marriage and 317,809 were registered outside of marriage. Since 2009, there has been a National increase in the number of live births registered within a same sex couples. In 2017 1,137 live registered births were recorded within a same sex marriage, whilst 450 were registered outside of marriage.
Gender Reassignment	No local data available. The Home Office 'Report of the interdepartmental working group on transsexual people' based on research from the Netherlands and Scotland, estimates that there are between 1,300 and 2,000 male to female and between 250 and 400 female to male transsexual people in the UK. However, Press for Change estimate the figures at around 5,000 post-operative transsexual people. Further, GIRES (2008) claims there are 6,200 people who have transitioned to a new gender role via medical intervention and approximately 2,335 full Gender Recognition Certificates have been issued to February 2009.
Marital Status	No local data available. There were 239,020 marriages between opposite-sex couples in 2015, a decrease of 3.4% from 2014 when there 247,372 marriages, and 0.8% lower than in 2013. Marriage rates for opposite-sex couples in 2015 were the lowest on record, with 21.7 marriages per thousand unmarried men and 19.8 marriages per thousand unmarried women. Compared with 2005, marriage rates for opposite-sex couples marrying in 2015 were lower at all ages, except for men aged 65 and over and women aged 55 and over where marriage rates increased. In 2015 there were 6,493 marriages between same-sex couples, 56% were between female couples; a further 9,156 same-sex couples converted their civil partnership into a marriage. In 2015, civil ceremonies among opposite-sex couples decreased by 1.6%, while religious ceremonies decreased by 8.0% compared with 2014. Same-sex couples mostly solemnised their marriages in civil ceremonies; there were only 44 religious ceremonies accounting for 0.7% of all marriages of same-sex couples. In 2015, of all individuals marrying a same-sex partner, 85% were forming their first legally recognised partnership compared with 76% for opposite-sex couples.
Age	Based on 2019 estimates, North Lincolnshire's proportion of older people (pensionable age) represents a higher percentage of the total population (21.3%) than seen in Yorkshire and Humber (18.8%) and England (18.4%). The working age population is less (60.2%) than that estimated in the Yorkshire and Humber region (62.1%) or over England as a whole (62.4%). North Lincolnshire's proportion of children represents a lower percentage of the total population (18.5%) than seen in Yorkshire and Humber (19.1%) and England (19.2%). In 2016, the median age of North Lincolnshire residents was 43.8 years, compared with 40 years nationally. North Lincolnshire already has a larger than average population of people aged 65+, and between 2019 and 2043 the 65+ population is projected to grow by a further 37%. Overall, the latest (2018) projections indicate a rise of 3.3% over the next 24 years, from an estimated 172,607 in mid-2019 to 178,336 in mid-2043. The projected

	increase in population in North Lincolnshire is not consistent across the age bands: the population aged 0-14 is projected to decrease by 12.1% from 30,101 in 2019 to 26,456 in 2043; the working age population is projected to decrease by 4% from 105,855 to 101,786; the 65+ population is expected to increase by 37% from 36,651 to 50,095. This age profile, combined with outward migration of working age adults and rising life expectancy, means that the number of people aged 80+ who are most vulnerable to frailty in older age is increasing faster in North Lincolnshire than nationally.

Equality Data

Is any equality data available relating to the use or implementation of this policy, project or function?	No
List any consultation e.g. with employees, service users, Unions or members of the public that has taken place in the development or implementation of this policy, project or function.	
Promoting inclusivity; How does the project, service or function contribute to our aims of eliminating discrimination and promoting equality and diversity?	

Equality Impact Risk Assessment test

What impact will the implementation of this policy, project or function have on employees, service users or other people who share characteristics protected by *The Equality Act 2010*?

Protected Characteristic:	No Impact	Positive Impact	Negative Impact	Evidence of impact and if applicable justification where a *Genuine Determining Reason* exists
Gender (Men and Women)	X			
Race (All Racial Groups)	X			
Disability (Mental and Physical, Sensory Impairment, Autism, Mental Health Issues)	X			
Religion or Belief	X			
Sexual Orientation (Heterosexual, Homosexual and Bisexual)	X			

Pregnancy and Maternity	X			
Transgender	X			
Marital Status	X			
Age	X			

Action Planning

As a result of performing this Equality Impact Analysis, what actions are proposed to remove or reduce any risks of adverse outcomes identified on employees, service users or other people who share characteristics protected by The Equality Act 2010?

Identified Risk:	Recommended Action:	Responsible Lead	Completion Date	Review Date

SUSTAINABILITY IMPACT

Staff preparing a Policy / Board Report / Committee Report / Service Plan / Project are required to complete a Sustainability Impact Assessment. Sustainability is one of the Trust's key Strategies and the Trust has made a corporate commitment to address the environmental effects of activities across Trust services. The purpose of this Sustainability Impact Assessment is to record any positive or negative impacts that this activity is likely to have on each of the Trust's Sustainability Themes.

	Positive Impact	**Negative Impact**	**No Specific Impact**	**What will the impact be? If the impact is negative, how can it be mitigated? (action)**
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			**X**	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			**X**	
Reduce the risk of pollution and avoid any breaches in legislation.			**X**	
Goods and services are procured more sustainability.			**X**	
Reduce carbon emissions from road vehicles.			**X**	

Reduce water consumption by 2020.			**X**	
Ensure legal compliance with waste legislation			**X**	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			**X**	
Increase the amount of waste being recycled to 40%.			**X**	
Sustainability training and communications for employees.			**X**	
Partnership working with local groups and organisations to support sustainable development.			**X**	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			**X**	