NHS
Nottingham and Nottinghamshire
Clinical Commissioning Group

Information Security Policy

2021–2024

Version:	3.0
Approved by:	Audit and Governance Committee
Date approved:	August 2021
Date of Issue (communicated to staff):	September 2021
Next review date:	August 2024
Document Sponsor:	Associate Director of Governance

CONTROL SECTION			
Reference Number IG-003	**Version** 3.0	**Status** FINAL	**Authors** Head of Information Governance Information Governance Delivery Manager
			Sponsor Associate Director of Governance
			Team Information Governance

Title	Information Security Policy		
Amendments	Update to v3.0 to include: • Reorganisation of sections. • Additional content added for clarity, completeness and explicitness; changes to meet DSPT and legal requirements. • Legal and Regulatory Framework inserted at Section 5. • Sections 5 and 6 reorganised and additional content: assets, pseudonymisation, data at rest, data protection by design, new information systems or changes to existing information systems. • Section 7 added – confidential data in the home or work environment. • Access controls grouped together into one section. • Section 9 added – IT Equipment Security. • Definitions of Terms inserted.		
Purpose	To provide a clear description of the responsibilities in respect of information, information systems and the security of these.		
Superseded Documents	Information Security Policy v1.1 and v2.1 DRAFT		
Audience	All employees of Nottingham and Nottinghamshire CCG (including all individuals working within the CCG in a temporary capacity, agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the CCG under contract for services), individuals appointed to Governing Bodies, Committees and any other individual directly involved with the business or decision-making of the CCG.		
Consulted with	Information Governance Steering Group, Associate Director of Governance		
Equality Impact Assessment	April 2021		
Approving Body	Audit and Governance Committee	**Date approved**	August 2021
Date of Issue	September 2021		
Review Date	August 2024		

This is a controlled document and whilst this policy may be printed, the electronic version available on the CCG's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.

Nottingham and Nottinghamshire CCG policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnccg.team.communications@nhs.net

Contents

1. Introduction

1.1 This document defines the Information Security Policy for Nottingham and Nottinghamshire CCG (subsequently referred to in this document as 'the CCG') and applies to all business functions and information systems, networks, physical environment and relevant people who support those business functions.

1.2 Information, in all its forms, is crucial to the effective functioning and good governance of the CCG and it is committed to efficient and effective information management and information security to ensure that all information and information systems, on which the CCG depends, are adequately protected. Information, paper and electronic systems, applications and the networks that support it are important organisational assets.

1.3 An information asset can be a single significant document or a set of related data, documents or files; it can be shared or confined to a specific purpose of a CCG function, service or business area. It could be operating systems, infrastructure, business applications, off-the-shelf products, services, policies, business continuity plans, records and information. It can be stored in computers, networks, printed out, written down, transmitted across networks and spoken in conversations.

1.4 Information security covers the policies and procedures in place to protect information and information systems from unauthorised access, use disclosure, disruption, modification or destruction. It is one of the fundamental components of the CCG's Information Governance Management Framework (IGMF) as it will ensure the confidentiality (security), integrity and availability of the CCG's information and Information Assets which also links to the CCG's Risk Management framework.

1.5 This document sets out the CCG's policy for the protection or security to ensure the confidentiality, integrity and availability of its information and information assets.

2. Legal and Regulatory Framework

2.1 This Information Security Policy is a requirement of the Data Security and Protection Toolkit (DSPT) that reflects the National Data Guardian's National Data Security Standards. This policy is a core policy that supports the CCG's IGMF which is based upon the legal requirements set out in the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), the Common Law Duty of Confidence, the Human Rights Act 1998, DSPT requirements and other related legal references and guidance.

2.2 This Information Security Policy must be read in conjunction with other supporting core policies and procedures to support this including the CCG's Confidentiality and Data Protection Policy, the Records Management Policy and the NHIS Network Security Policy.

3. Policy Aims

3.1 The objective of this policy is to enable the CCG to protect its information assets by:

- Setting out a framework for information security.
- Promoting a culture of information security best practice across the CCG and its partners.
- Ensuring staff understand their responsibilities.

3.2 Application of the Information Security Policy will ensure that:

- The CCG's Governing Body has appointed an approved Senior Information Risk Owner (SIRO).
- Each Information asset has been assigned an Information Asset Owner (IAO) who is responsible for ensuring the risk assessment of those assets in order to be able to provide assurance to the SIRO that:
    - Information is protected against unauthorised access and/or misuse.
    - The confidentiality of information is assured.
    - The integrity of information is maintained.
    - Information is available where and when required.
    - Business Continuity Plans are produced, maintained and tested.
    - Regulatory, legal and contractual requirements are complied with.
    - Appropriate training is provided to all staff.
    - Breaches of information security, confidentiality and data protection are reported and investigated.

- The physical and environmental aspects of information security are considered and managed.
- Any new or changes to existing information assets are reviewed by IAOs for any data protection implications through the use of Data Protection Impact Assessments (DPIAs).

4. Scope

4.1 The Information Security Policy covers the protection of all forms of information to include its confidentiality (security), integrity and availability and applies to:

- All staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the CCG.

- All systems and applications attached to CCG information systems and computer networks. The term 'information asset' refers to IT infrastructure and operating systems, business applications, off-the-shelf software products, services of specialist staff, user-developed applications (e.g. databases), hard-copy (paper) records and electronic data. The term can also apply to knowledge and intellectual property.

- All information (data), personal and sensitive personal (special category) information processed by the CCG pursuant to its operational duties and activities, regardless of whether it is processed in electronic or in paper (hard copy) form, any communications sent to or from the CCG and any CCG information (data) held on systems external to the CCG's network.

- All external parties with access to CCG information systems, that provide services to the CCG in respect of its processing and business functions.

- All electronic and paper information assets including all the physical locations where assets are held or where the CCG operates from.

4.2 The policy is applicable to all areas of the organisations and adherence should be included in all contracts for outsourced or shared services, without exclusion.

4.3 This Policy covers:

Systems and Devices

- All manual and electronic information systems owned, operated or managed by the CCG or NHIS including networks and application systems, whether or not such systems are installed or used on CCG premises.

- Other systems brought onto CCG premises including, but not limited to, those of contractors and third party suppliers, which are used for CCG business.

- Desktop devices used to hold CCG information such as laptops and PCs, tablets and mobile phones.

- Removable media, such as USB memory sticks and external hard drives.

Information

- All information collected or accessed in relation to any CCG activity whether by CCG employees or individuals and organisations under a contractual relationship with the CCG.

- All information stored on facilities owned, leased or managed by the CCG or on behalf of the CCG.

- Information stored and processed manually and electronically by the CCG including the transmission, printing, scanning of that information.

- Information processed by a contractor organisation on the CCG's behalf and which is held on non–CCG premises.

- Information identified as structured data (organised and formatted) or unstructured data (no pre-defined format or organisation).

It is the responsibility of all individuals with access to information to adhere to this policy and all relevant policies that maintain the 'confidentiality (security), integrity and availability' of information systems and the confidential information processed within them.

Failure to adhere to this policy may result in disciplinary action and where necessary, referral to the appropriate regulatory bodies including the police and any relevant professional bodies.

5. Accountability and Responsibility

5.1 This policy forms part of the CCG's Information Governance and Management Framework (IGMF). There are a number of key information governance roles, committees and groups that the CCG needs to have in place as part of the IGMF. These are:

- CCG Governing Body.
- Audit and Governance Committee.
- Information Governance Steering Group.
- Senior Information Risk Owner (SIRO).
- Caldicott Guardian.
- Data Protection Officer.
- Associate Director of Governance.
- Information Asset Owners (IAOs).
- Information Asset Administrators (IAAs) or Information Asset Manager (IAM).
- Heads of Service.
- All employees.

5.2 The accountability and responsibilities are set out in more detail in the IGMF which must be read in conjunction with this policy. Achieving IGMF objectives depends on staff and partners working within the CCG's policies, legislation, regulations and best practice guidelines and it is the responsibility of all individuals, with access to CCG information, to adhere to the requirements set out in this policy and all relevant policies that maintain the 'confidentiality (security), integrity and availability' of information systems and the personal and confidential data processed within them.

6. Organisational Information Security Requirements

Information Systems or Assets

6.1 Business function information systems of confidential, personal or special category data are information assets and must be recorded by IAOs on their business area Information Asset Register (IAR) as part of the CCG's Information Asset Management which supports the CCG's responsibilities under Data Protection Article 30 to hold a Record of Processing Activities (RoPA). These assets will include risk assessments and business continuity planning.

6.2 IAOs are responsible for ensuring the confidentiality, integrity and availability (i.e. security) of information systems for which they are responsible, which includes physical and environmental security.

6.3 For information that does not contain personal or confidential details, staff will still need to process these records securely. Access to these types of records by staff or by partner organisations will be dictated by a staff member's authorised and agreed duties for organisational business needs. Access in the wider context such as in the public domain will be dependent on legislative requirements.

Anonymised Data

6.4 Anonymisation is the process of removing personal identifiers, both direct and indirect, to prevent an individual from being identified. Once data is truly anonymised individuals are no longer identifiable and anonymisation can form part of information security measures.

Pseudonymised Data

6.5 Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. This process de-identifies data making it less likely that individuals can be identified. Pseudonymisation involves replacing personal data with other values or a pseudonym which can be reversed by the original body that carried out the pseudonymisation. Once data is truly pseudonymised individuals are no longer identifiable without access to additional information and anonymisation can form part of information security measures.

Data at Rest

6.6 Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Information security aims to secure inactive data stored on any device or network. The information security risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.

Data in Transit

6.7 Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. When transferring information, staff must take into account the nature of the information to be transferred and ensure that it has the necessary protection to ensure its security. This is especially important when information contains personal or special categories of personal data. The paragraphs below set out different types of data transfer and security requirements.

Non Routine Bulk Transfers

6.8 Any non-routine bulk extracts ("bulk" is defined as 50+ records) or transfers of personal confidential or sensitive data must be authorised by the responsible manager or the IAO for the work area and may require approval by the SIRO – contact the IG Team for further advice – nnccg.ig.greater-nottingham@nhs.net

Transfer by FAX

6.9 Transfers of personal or special categories of data by fax have been banned by the NHS as of 31 March 2020.

Data Transfer outside EEA

6.10 Consult with the IG Team when considering any transfer of personal or special categories of data outside the EEA to ensure security of the information. Specific legal requirements are required for such transfers. Care must be taken when procuring new systems to ensure the geographical location of data is known and the risks appropriately assessed.

Data Protection by Design

6.11 Article 25(1) of the GDPR places two key obligations on data controllers when designing products and services to (1) implement appropriate technical and organisational measures that are designed to implement the data protection principles (Article 5) and (2) integrate necessary safeguards. In order to implement these data protection requirements, the CCG is required to ensure Data Protection by Design by evaluating the risks of varying likelihood and severity for the rights and freedoms of natural persons, posed by the processing of their personal data.

6.12 The CCG's approach to Data Protection by Design is set out in the document 'IG-PRG-008 Data Protection by Design Framework'. Carrying out a Data Protection Impact Assessment (DPIA) is an important part of this Privacy by Design approach to ensure from the earliest point in project planning that consideration has been afforded to privacy and data protection aspects of the work.

New Information Systems or changes to existing Information Systems

6.13 Where a new information system is considered for introduction or there are to be changes made to an existing system, the CCG will engage with NHIS IT security expertise to ensure that any new system meets information security requirements. An assessment to meet the Digital Technologies Assessment Criteria (DTAC) which is a support tool introduced by NHSX in 2021 may be required.

6.14 An IAO will need to be identified and a DPIA will be required as part of any overall project plan that involves the processing of personal data. This will enable any privacy and/or security risks or issues to be identified so that these can be addressed before any project goes ahead that may be unlawful.

6.15 Specific measures and procedures need to be in place to ensure the system is lawful and secure and this includes:

- Effective security counter measures.
- Relevant security documentation.
- Security operating procedures.
- Security contingency plans.

6.16 The IAO will have responsibility for the security of designated information assets and needs to be aware of and in agreement with any proposed changes to an existing system or where a new system is being introduced.

6.17 IAOs will need to assure the SIRO through the DPIA and any other relevant documentation (e.g. contracts/data processing/information sharing agreements) that the changes or introduction of a new system comply with legislation and that the necessary technical and organisational measures are in place to ensure security. The IAO must update the IAR when changes are made to existing systems or a new system is introduced. The CCG's IAR is a record of all key information assets and held by the CCG's IG Team.

6.18 For any new IT supplier or organisation processing data on the CCG's behalf, due diligence must be carried out to ensure the necessary standards are being met and appropriate certification is in place. Any identified data security risks will be addressed ahead of any contract award. Contracts in place must contain the necessary clauses around privacy, confidentiality and compliance with appropriate security policies.

7. Confidential Data – Physical/Electronic Security

7.1 In order to minimise loss of or damage to personal or special category personal data and information assets, all information storage equipment and areas must be physically and technically protected from information security threats and environmental hazards.

7.2 Personal and confidential information must not be stored on unauthorised and unencrypted local or removable hard drives such as PC removable hard drives, laptops, USB sticks or other portable devices.

7.3 Any personal, confidential or special category data held on portable media devices must only be held on authorised devices and be encrypted to the minimum required standards for NHS.

7.4 Only authorised individuals with specific need will have administrative and privileged access to manage IT network functions including user support and account management. Privileged Access management controls will be in place and identified individuals will adhere to explicit codes of conduct, terms and conditions.

Confidential Data in the Home or Work Environment

7.5 All employees have a responsibility to ensure they keep personal and confidential data they use in their roles secure and protected from unauthorised access. Hard copy documents should be locked away and electronic records stored in secure folders on the network protected by password, device lock and other appropriate security.

Guidelines for securing personal confidential data should be followed (see **Appendix B:** 'Good Practice Guide - Physical and Electronic Information Security').

8. Access Controls

Role Based and Authorised Access Control

8.1 The CCG employ role based and authorised access controls following the principle of least privilege.

8.2 Access to information and information systems, whether electronic or manual, is restricted to authorised users who have an identified need as agreed with their line manager, sponsor and/or IAO.

8.3 Access to electronic information systems is given at the appropriate level for the agreed need by the appropriate IAO.

8.4 Access to confidential information is given at an appropriate level taking into account and the level of authorised access to personal and personal special category data. Staff should only have access to the data necessary for the completion of the business function. This can include access that is restricted to anonymised or pseudonymised personal data.

8.5 Smart cards are used for access to some systems such as ESR and some patient systems. Users must follow the Smart Card Policy.

8.6 IAOs must review whether staff should have access (or be granted access) to an information system. This process needs to be recorded and included in their IAR against the appropriate information asset in support of the CCG's IAR or Record of Processing Activities (RoPA).

8.7 Where staff members leave or move to another section, line managers are responsible for informing IT Services (NHIS) and IAOs of the change so that access to any relevant information systems is revoked by the IAO where that access is no longer justified.

8.8 Personal and special categories of data may only be stored within a secure environment on operational systems within a safe haven i.e. there is restricted access and technical security relative to the sensitivity of the information.

Electronic Access Control – Password Protection

8.9 The primary form of access control for the CCG's computer systems is via individual log-in and password. Each member of staff using a computer system will have an individual log-in account and password. Sharing of passwords and use of those passwords can be classed as an offence under the Computer Misuse Act 1990. All staff must follow robust security practices in the selection and use of passwords. Logon details are not to be shared or used under supervision, even in training situations. Staff will be held responsible for any action undertaken with their login credentials.

8.10 **Email and Internet Security**

See the CCG's Internet and Email Policy.

Physical Access Control

8.11 Only authorised personnel who have an identified need will be given access to restricted areas containing information systems such as the server room or a file store room.

8.12 Confidential information held in hard copy (paper) must be kept secure at all times e.g. locked in a cabinet when not in use.

8.13 There will be appropriate access controls in place at CCG premises e.g. access to the building controlled by proximity device, code entry, or reception controlled access.

8.14 Non-CCG staff need to sign in at the CCG's reception register when working on CCG premises and must be accompanied by a member of CCG staff at all times.

8.15 All staff should wear an identification badge at all times when on CCG premises.

8.16 Staff should challenge individuals where appropriate who they do not recognise, do not have an ID badge and who do not appear to be working for or with any particular section or team. Unauthorised individuals must not be allowed to tailgate into secure premises or locations. Where there is any behaviour by an individual who seems suspicious and who may be interpreted to present any threat to an individual, they should report this to the building's security/reception without delay.

Access to Generic Network Accounts

8.17 The use of one account used by more than one individual can present a heightened security risk. However on occasion the use of a generic account is the most logical business option.

8.18 Should a generic account be required, it must follow guidance for use of generic accounts, have line management approval, IT risk assessment and IG Team sign off.

8.19 All generic accounts must be managed as information assets, i.e. recorded, assigned ownership and managed in accordance with information asset management protocols and data protection requirements.

8.20 Generic accounts for information systems must be considered and approved on a case-by-case basis with IG Team and DPO appraisal and authorisation.

8.21 Generic email accounts should follow the CCG's Internet and Email Policy.

Access to National Applications Systems

8.22 National applications include systems, services and directories that support the NHS in the exchange of information across national and local NHS systems e.g. Summary Care Record, e-Referrals, Electronic Staff Records. In some cases these involve access to patient healthcare information. National Spine-enabled systems are controlled by a number of different security mechanisms (these are listed below).

8.23 The CCG is a commissioner of healthcare services and not healthcare providers and will only have access to patient healthcare information for very limited purposes and where there is a legal basis (see Health and Social Care Act 2012). For example, there is a recognised legal basis for the processing of Personal Confidential Data for Continuing Healthcare, Individual Funding Requests, complaints, managing incidents and medicines optimisation/management.

8.24 The types of personal information accessed by the CCG are set out in the Privacy Notice on the CCG's website. The range of access controls applied by national applications include:

- **Smart Card:** Access will be restricted through the use of a NHS Smart card with a pass code, provided by the local Registration Authority.
- **Legitimate relationships**: Staff will only be able to access patient records if they are involved in that patient's care.
- **Role Based Access Control (RBAC)**: Access will depend on staff roles/ job/position functions. Roles and access privileges will be defined centrally and given locally by staff designated to do this in the organisation.
- **Audit trails**: An electronic record will be made automatically of who, when and what information a user accessed and/or edited. Trails can be assessed by an appropriately authorised manager.
- **Alerts**: Alerts will be triggered automatically both to deter misuse of access privileges and to report any misuse when it occurs.

Access to IT Networks

8.25 This is covered in CCG's IT Services provider, NHIS's Network Security Policy which should be read in conjunction with this policy.

Remote Working

8.26 Work-related information that is taken off-site must be authorised by line management, protected by proper security and, where held on portable computers or devices be encrypted and backed up regularly to the appropriate CCG server. Portable computers or devices must be used in line with CCG procedures and protected by appropriate security and encryption. Staff should refer to leaflet 'IRG-PRG-006 Electronic Remote Working', for further information. It is recognised that remote access to the network provides an option whereby the need to transport information manually is removed. Working remotely must comply with the full suite of policies relating to Information Governance.

9. IT Equipment Security

Portable Devices

9.1 The use of work-issued portable devices (which includes laptops, mobile phones, smart phones/tablets, USB memory sticks) must be used in line with CCG policy and authorised by line management and the CCG IT Services provider, NHIS, where appropriate.

9.2 Using work–issued portable devices ensures that the requirements of this policy and all CCG and NHS requirements for the security of portable computers and device usage are met.

9.3 Work-issued devices must only be used by the individuals to whom they were issued.

9.4 All work-issued portable devices, including those which are able to store data, must be encrypted to meet information classification requirements such as the National Cyber Security Centre (NCSC) guidance for OFFICIAL data (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf) and, where appropriate, have up-to-date antivirus software.

9.5 Wherever available, security features such as passwords and encryption should be used on all devices. As a minimum, for example, a 4-digit PIN should be used on a mobile phone to prevent any unauthorised access.

9.6 Any exceptions to this policy for portable devices must be risk assessed and approved by the CCG Information Governance Team and NHIS Information Security specialists.

9.7 When staff leave the CCG, they must return any equipment provided by the CCG.

Secure Disposal and Re-use of Equipment

9.8 All users must ensure that, where equipment is being disposed of, all data on the equipment (e.g. on hard disks or removable media) is securely destroyed; this can be arranged through NHIS. Equipment must be assessed for re-use before being given to a new user or being disposed of. For disposal of paper records see the CCG's Records Management Policy.

Use of Personal Devices

9.9 Whilst the CCG does not have a Bring Your Own Device (BYOD) policy, it is accepted that on occasion in exceptional circumstances and for limited purposes, staff may use personal devices (non-work issued devices) for work purposes such as accessing NHSmail email or non-confidential work documentation sent via email (secure email where possible). Where individuals use personal devices such as mobile/smart phones, laptops, tablets etc., for these reasons, they must follow the relevant CCG policies.

9.10 Whenever staff choose to access NHSmail this way, they should only do so in accordance with NHSmail guidance. Only access through an approved work-issued device should be performed through the "private" setting. Otherwise

this option should not be selected which provides security through prevention of any download of data to the device.

9.11 Personal devices (non-work issued devices) must not be used to routinely store personal or confidential work related or acquired data.

9.12 Personal devices (non-work issued devices) must not be directly connected to the corporate network either by a direct network cable connection or Wi-Fi connection without appropriate IG and IT approval.

9.13 Any software or applications on personal devices should not be used for work purposes unless approved by NHIS and CCG Information Governance.

10. Network Security

Malicious and Unauthorised Software

10.1 This is covered in NHIS's Network Security Policy which must be read in conjunction with this Policy.

10.2 All portable data storage devices (including CDs, DVDs, USB and flash drives) containing software or data from external sources, or that have been used in external equipment, must be authorised and fully virus checked before being used on the CCG network. NHIS can provide appropriate advice on such matters.

Internet Use

10.3 See the CCG's Internet and Email Policy.

Cloud Use

10.4 Any services employed that utilise Cloud online storage must be verified as secure. Personal, confidential data must not be stored in cloud services not verified as meeting necessary security standards. Any staff wanting or needing to use such services for business purposes must obtain the necessary security assurance from NHIS and authorisation from the IG Team. Users can refer to the National Cyber Security Centre's (NCSC) 14 Cloud Security Principles; 'IG-NHIS-006-Using the Cloud - Procedure' and 'IG-NHIS-007- Cloud Guidance'.

Network Technical Compliance Checking

10.5 The SIRO will seek assurance from the CCG's IT Provider, NHIS, that information systems are regularly checked for compliance with security implementation standards.

11. Organisational Controls

Monitoring System Access and Use

11.1 Where possible, audit trails of system access and use should be maintained and reviewed on a regular basis by the associated IAO.

Business Continuity

11.2 The CCG will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks in order to comply with the 'availability' information security requirement. These form part of the CCG's formal Business Continuity Plans.

Information Security Incident Reporting

11.3 All information management and technology security incidents and weaknesses must be reported immediately via the CCG's incident reporting procedures set out in the CCG's Incident Reporting and Management Policy which is available on the CCG website.

11.4 All security incidents resulting in an actual or potential breach of confidentiality must be reported in accordance with policies and procedures including notification to Information Governance, the SIRO or Caldicott Guardian as appropriate within 24 hours of identification. For serious incidents, the CCG has a legal obligation to report externally to the ICO within 72 hours, so staff must not delay in notifying suspected or actual breaches.

11.5 Any Information Governance related incident, especially related to a breach of GDPR or Data Protection Act, must be reported in line with the CCG's Incident Reporting and Management Policy. The personal data breach grading on DSPT guidance should be completed for every incident reported, this will enable to IG Team to assess the severity of the incident.

11.6 Examples of data breach are when there is a loss of personal or special category data involving individuals or where sensitive personal information is lost (unrecoverable) or sent to the wrong address. Staff must read the CCG's Incident Reporting and Management Policy for general reporting of incidents and the process for Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Incident Investigation - Forensic Readiness

11.7 Forensic readiness is a key component in the management of information risk. It describes an organisation's ability to investigate computer equipment usage retrospectively, using digital evidence, without compromising the integrity of that evidence.

11.8 The CCG may need to recover and analyse digital evidence as part of an investigation. To ensure the availability, reliability and admissibility of that evidence in a situation where it has to be produced in a legal case or disciplinary hearing, it should be recovered and analysed in a manner that:

- Is systematic, standardised and legal, in order to protect the CCG and staff.
- Allows consistent, rapid investigation of major events or incidents with minimum disruption to the organisation's business.
- Enables the proactive and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required.
- Demonstrates due diligence and good governance of the organisation's information assets.

11.9 The organisation's IAOs are responsible for ensuring that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned 'ownership' and includes:

- Ability to gather digital evidence without interfering with business processes.
- Prioritising digital evidence gathering to those processes that may significantly impact the organisation, its staff and its patients.
- Allow investigation to proceed at a cost in proportion to the incident or event.
- Minimise business disruptions to the organisation.
- Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action.

11.10 Digital evidence may feature in investigations or disputes involving CCG information that includes, but is not confined to:

- Patient confidentiality breaches and complaints requiring investigation.
- Security incidents such as unauthorised access to, tampering with or use of IT systems, electronic attack, including denial of service and malicious software ('malware') attacks (e.g. viruses, worms, Trojan).
- Criminal activities such as fraud, deception, money laundering, threats, blackmail, extortion, harassment, stalking.
- Commercial disputes such as those involving intellectual property rights.
- Disciplinary issues including accidents, negligence, malpractice, abuse of the CCG's Internet and Email policy or other Information Governance policies.
- Privacy issues such as identity theft, invasions of privacy, non-compliance with the Data Protection Act and other relevant legislation.

11.11 The Associate Director of Governance/Head of Information Governance **must** be notified in the first instance where a requirement for a forensic investigation has been identified and before it is instigated.

11.12 The CCG's Local Counter Fraud Service will be contracted to undertake any forensic investigations.

11.13 The SIRO is responsible for co-ordinating any forensic investigation for the organisation.

12. Training

12.2 Information governance and security will be a part of induction training and is an annual mandatory training requirement for all staff. The information governance training needs of key staff groups is specified in the IG Training Plan, which takes into account roles, responsibilities and accountability levels. It is a line management responsibility to ensure that all staff are made aware of their information security responsibilities through generic and specific staff training.

13. Information Security Risk Management

13.1 Data Protection Impact Assessments (DPIAs) completed post-information incident will identify the appropriate security counter measures necessary to protect against possible breaches of privacy, confidentiality, integrity and availability. Once identified, information security risks shall be managed on a formal basis.

13.2 They shall be recorded within the CCG's risk register and action plans shall be put in place to effectively manage any identified privacy, confidentiality, integrity and availability risks. Additionally, assurance is provided to the SIRO via the CCG's IAR which records that information security risk assessments for assets have taken place. The CCG's Risk Management Policy should be read in conjunction with this section.

14. Communication, Monitoring and Review

14.1 Following endorsement by the Information Governance Steering Group and ratification by the Audit and Governance Committee, this policy will be communicated and disseminated to staff via the CCG's staff bulletin and placed on the CCG's Website.

14.2 An assessment of compliance with requirements, within the Data Security and Protection Toolkit (DSPT), will be undertaken each year. This includes Confidentiality and Data Protection. All serious information governance incidents will be reported by the SIRO at Governing Body level and in Annual Reports. Incidents will be reported and learning from incidents implemented at the Information Governance Steering Group.

14.3 This Policy will be reviewed every three years or in line with changes to relevant legislation, national guidance or other significant requirements.

14.4 Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the document author.

15. Associated Documentation

15.1 The CCG will produce appropriate policies, procedures and guidance relating to records management as required. This will include the 'IG-PRG-002 Information Governance Staff Handbook' which will be updated annually and which will be provided to all staff. This policy should be read in conjunction with the following:

- GOV-001 Risk Management Policy
- GOV-006 Emergency Preparedness, Resilience and Response Policy
- GOV-008 Incident Reporting and Management Policy
- IG-001 Information Governance Management Framework
- IG-002 Confidentiality and Data Protection Policy
- IG-004 Internet and Email Policy
- IG-005 Data Quality Policy
- IG-006 Records Management Policy
- IG-007 Freedom of Information and Environmental Information Regulations Policy
- IG-PRG-001 Safe Haven Procedure
- IG-PRG-002 Information Governance Staff Handbook
- IG-PRG-003 IG Code of Conduct
- IG-PRG-004 DPIA Template and Guidance
- IG-PRG-005 Information Asset Management Procedure
- IG-PRG-006 Electronic Remote Working Leaflet
- IG-PRG-007 SAR – Information Rights Procedure
- IG-PRG-008 Data Protection by Design Procedure
- IGNHIS-001 Smart Card Policy
- IGNHIS-002 NHIS Network Security Policy
- IGNHIS-003 NHIS Acceptable Use Policy
- IGNHIS-004 NHIS Removable Media Policy
- IGNHIS-005 NHIS Patch Management Policy
- IGNHIS-006 NHIS Cloud Storage
- IG-PRG-007 NHIS Cloud Guidance.

16. Legal References and Guidance

- Access to Health Records Act 1990
- Audit & Internal Control Act 1987
- Bribery Act 2010
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Data Protection Act 2018
- EU General Data Protection Regulation 2016
- Electronic Communications Act 2000
- Enterprise and Regulatory Reform Act 2013
- Environmental Information Regulations 2004
- Equality Act 2010
- Fraud Act 2006
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- NHS Digital Guidance
- Human Rights Act 1998
- Information Commissioner's Guidance Documents
- ISO/IEC 27001:2005 Specification for an Information Security Management System
- ISO/IEC27002:2005 Code of Practice for Information Security Management
- NHS Act 2006
- NHS Information Security Management Code of Practice 2007
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Privacy and Electronic Communications Regulations 2003
- Professional Codes of Conduct and Guidance
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulations under Health and Safety at Work Act 1974
- The Children Act 1989
- UK GDPR
- 2004 Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992.

17. Equality and Diversity Statement

17.1 The Nottingham and Nottinghamshire CCG pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, both as a commissioner and as an employer.

17.2 As a commissioning organisation, the CCG is committed to ensuring its activities do not unlawfully discriminate on the grounds of any of the protected characteristics defined by the Equality Act, which are age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

17.3 The CCG is committed to ensuring that commissioning activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, roma and travellers.

17.4 As an employer, the CCG is committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

17.5 To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

18. Equality Impact Assessment

Date of assessment:	April 2021			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age[1]	No	N/A	N/A	N/A
Disability[2]	Yes	Mechanisms are in place via the Communications and Engagement Team to receive the policy in a range of languages, large print, Braille, audio, electronic and other accessible formats.	No	
Gender reassignment[3]	No	N/A	N/A	
Marriage and civil	No	N/A	N/A	

[1] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).
[2] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.
[3] The process of transitioning from one gender to another.

Date of assessment:	April 2021			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
partnership[4]				
Pregnancy and maternity[5]	No	N/A	N/A	
Race[6]	No	N/A	N/A	
Religion or belief[7]	No	N/A	N/A	
Sex[8]	No	N/A	N/A	
Sexual orientation[9]	No	N/A	N/A	
Carers[10]	No	N/A	N/A	N/A

[4] Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[5] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

[6] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

[7] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

[8] A man or a woman.

[9] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[10] Individuals within the CCG which may have carer responsibilities.

Appendix A

Definitions of Terms

Anonymisation	The act of permanently removing identifying characteristics from personal data. Compare *pseudonymisation*.
Cloud	"The **cloud**" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. ... By using **cloud** computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines.
Cyber Attack	A cyber-attack is the deliberate exploitation of computer systems, technology-dependent enterprises and networks.
Cyber Security	Cyber Security Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them.
DPIA	A Data Protection Impact Assessment (**DPIA**) is a process to help identify and minimise the data protection risks of a project. ... identify and assess risks to individuals; and identify any additional measures to mitigate those risks.
DSPT	Data Protection and Security Toolkit (the Toolkit) is the annual NHS Digital IG self-assessment tool for NHS organisations.
Forensic Readiness	The achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law.

Information Asset	Any information that is stored physically or electronically, transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed.
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
National Data Guardian's National Data Security Standards	10 Data Security Standards introduced by the National Data Guardian and upon which the DSPT (Toolkit) is now based.
Pseudonymisation	The act of making the identifiers of person identifiable data obscure to protect privacy e.g. use of pseudonym or alias or other non-identifying label. Data can be re-identified with the relevant knowledge or system. Compare *anonymisation.*
RoPA	A requirement as set out in Article 30 of the Data Protection Act for organisations processing personal data to maintain a list of specific data processing activities and information about those activities.
Safe Haven	A location which is set up to receive and manage confidential information appropriately. It may be a post room, reception area or fax machine or anywhere messages may be taken and held before being passed onto the appropriate recipient.
SIRO	Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. They ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

Appendix B

Good Practice Guide - Physical and Electronic Information Security

This section is intended to be a quick reference guide for staff on information security good practice. It lists some of the key areas of the Information Security Policy but is not intended to be a comprehensive summary and does not reduce or alter the standards or principles laid out in this policy. Additional guidance is available within the CCG's Information Governance Staff Handbook.

- **Confidential waste** - ensure confidential waste is locked away securely until collection. Never leave confidential waste bags in corridors/outside office doors for collection. Ensure appropriate destruction of confidential paper and electronically held information.

- **Clear desks** - make sure confidential information on your desk cannot be overlooked. Some offices are used by multiple staff for multiple purposes and therefore it is essential that desks are clear to avoid unauthorised disclosure of information.

- **Locked cabinets** - make sure cabinets with confidential information contained in them are locked and appropriate access controls are in place in terms of who holds the keys.

- **Access controls on electronic folders** - adopt the same principles as you would for paper records. Ensure only authorised staff have access to electronically held information. Where required password protect folders or individual documents saved on the shared drive.

- **Smart Cards** - never leave your smart card in your computer when you are away from your desk, this could potentially lead to a serious confidentiality breach given the personal and sensitive data which Smart Cards provide access to.

- **Office environments** - wherever possible, escort visitors on and off site. Always wear your identity badge and where appropriate, challenge people who you do not recognise. If you work in an open office ensure that private conversations take place in private meeting rooms.

- **Using the telephone** - when leaving messages, only leave the minimum required e.g. name and contact details. When sharing information on the telephone make sure you have identification processes in place to check who you are speaking to or if you are unsure, offer to call the person back, if possible, via a main switchboard.

- **Using a computer** – do not share passwords. Lock your computer when leaving your desk (ctrl-alt-del return keys). Do not let personal data on your screen be overlooked and do not let someone else use your computer when you are logged on. Ensure your mobile device is regularly connected to the network to ensure antivirus software is updated maintained.

- **Printing** - avoid printing personal/confidential information to shared/central printers. If you absolutely need to, make sure you collect it straight away. Keep printing to a minimum and always ensure your computer is networked to the correct printer.

- **Post** - ensure only items to be sent are included and nothing extra. Ensure confidential post is placed in a sealed envelope and marked ‘confidential’. Never use re-sealable envelopes for sending personal data. Make sure items are properly addressed to avoid mis-delivery and check receipt of critical items. For very sensitive or ‘bulk’ data consider if you need to send ‘special delivery’.