NHS
Leeds
Clinical Commissioning Group

Information Security Policy

Version:	2.1
Ratified by:	Audit Committee
Date ratified:	16 September 2020
Name & Title of originator/author:	Abi Dakin, Cyber Assurance and Compliance Manager
Name of responsible committee/individual:	Information Governance Committee
Date issued:	September 2020
Review date:	September 2022
Target audience:	All staff

Executive Summary

This document defines the Information Security Policy for NHS Leeds Clinical Commissioning Group (CCG).

It is intended to set out CCG policy for the protection of the confidentiality, integrity and availability of information assets including hardware, software and data handled by information systems, networks and applications. It also relates to paper-based information assets and verbal communications. The document establishes the security responsibilities of employees, systems and technical controls required to mitigate against risks to data security.

References are provided for other related documentation.

The Information Governance Policy and Management Framework acts as an overarching policy for the core information governance polices. The Information Security Policy is one of those core policies and must be read in conjunction with the overarching Policy. Additionally, procedures to support this policy should also be read in conjunction with the other information governance and security related policies including the Network Security Policy.

Equality Impact Assessment (EIA)

This document has been assessed, using the EIA toolkit, to ensure consideration has been given to the actual or potential impacts on staff, certain communities or population groups, appropriate action has been taken to mitigate or eliminate the negative impacts and maximise the positive impacts and that the and that the implementation plans are appropriate and proportionate.

Contents

1 Introduction 4

2 Aims 4

3 Objectives 5

4 Scope 5

5 Accountability and Responsibilities 5

6 Policy framework 6

6.1 Contracts of Employment 6

6.2 Security Control Assets 6

6.3 Access Controls 6

6.4 Computer Access and Application Controls 6

6.5 Equipment Security 7

6.6 Computer and Network Procedures 7

6.7 Information Risk Assessment 7

6.8 Information Security Events and Weaknesses 7

6.9 Protection from Malicious Software 7

6.10 Removable Media 7

6.11 Monitoring System Access and Use 7

6.12 Accreditation of Information Systems 8

6.13 System Change Control 8

6.14 Business Continuity and Disaster Recovery Plans 8

6.15 Training & Awareness 8

6.16 IG requirements for New Processes, Services, Information Systems and Assets 8

7 Distribution and Implementation 8

8 Monitoring 8

9 Associated Documentation 9

Appendix A Request for Equipment Retention During Long Term Absence 10

1 Introduction

NHS Leeds Clinical Commissioning Group (CCG) is a public body, with formation processing as a fundamental part of its purpose. It is important, therefore, that the organisation has a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and to ensuring that confidentiality is respected.

The purpose of this Information Security policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially it encompasses the behaviour of the people who manage information in the line of CCG business.

Information security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the CCG is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on CCG business.
- A strengthened position in the event of any legal action that may be taken against the CCG (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

2 Aims

Confidentiality	Access to Data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

3 Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the CCG:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Information Governance policies.
- Working with GPs who share a common Open Service supply partner, to develop collaborative approaches, systems and processes relating to information security.
- Describing the principles of security and explaining how they are implemented in the organisation. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

4 Scope

This policy must be followed by all staff who works 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. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

5 Accountability and Responsibilities

There are a number of key information governance roles and bodies that the CCG needs to have in place as part of its Information Governance Framework, these are:

- Governing Body
- Audit Committee
- Senior Information Risk Owner
- Caldicott Guardian
- Data Protection Officer
- Qualified Cyber Professional
- Information Asset Owners
- Information Asset Administrator
- Heads of Service
- All employees

The accountability and responsibility are set out in more detail in the Information Governance Policy and Management Framework which must be read in conjunction with this policy.

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

6 Policy framework

6.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions and descriptions

6.2 Security Control Assets

All IT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

It is the responsibility of all Line Managers to secure the return of the assets such as laptops, mobile phones or any other equipment provided by the CCG when the member of staff leaves the CCG or are on long term leave (see Starters, Movers and Leavers guidance). In exceptional circumstances, the Line Manager may apply for long term absentees to retain any CCG equipment during their absence. It is the Manager's responsibility to ensure that equipment is returned on request. See Appendix A Request for Equipment Retention

It is the responsibility of all leavers to comply with this request and should they fail to comply with their responsibilities, the escalation process is outlined in the Starters, Movers and Leavers guidance separately.

6.3 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO.

6.4 Computer Access and Application Controls

Access to data and system utilities shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

6.5 Equipment Security
In order to minimise loss of, or damage to, all assets, the IT Team shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

6.6 Computer and Network Procedures
Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of the CCG.

6.7 Information Risk Assessment
All information assets will be identified and assigned an Information Asset Owner (IAO).IAO's shall ensure that information risk assessments are performed at least annually,following guidance from the Senior Information Risk Owner (SIRO). IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review.

Please see the Information Asset Owners Guidance for further information.

6.8 Information Security Events and Weaknesses
All CCG information security events, near misses, and suspected weaknesses are to be reported on Datix and to the Information Governance team. All adverse incidents shall be reported to the CCG DPO. The Information Security Incident Reporting procedures must be complied with.

6.9 Protection from Malicious Software
The organisation and its IT service providers shall 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 shall not install software on the organisation's property without permission from the IT Manager or Head of IT & and Business Change. Users breaching this requirement may be subject to disciplinary action.

6.10 Removable Media
The CCG IT systems automatically encrypt removable media. Removable media that contain software require the approval of the Head of IT & and Business Change before they may be used on CCG systems. Users breaching this requirement may be subject to disciplinary action.

6.11 Monitoring System Access and Use
An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The CCG will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy.

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

6.12 Accreditation of Information Systems

The CCG shall ensure that all new information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the DPO/SIRO before they commence operation.

6.13 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the IT Manager.

6.14 Business Continuity and Disaster Recovery Plans

The CCG will implement a business continuity and disaster recovery plans. Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

6.15 Training & Awareness

Data Security and Protection training is mandatory and all staff are required to complete annual on-line or face to face workshop Data Security Awareness training.

6.16 IG requirements for New Processes, Services, Information Systems and Assets

The IG requirements for New Processes, Services, Information Systems and Assets procedure must be complied with when:

- A new process is to be established that involves processing of personal data (data relating to individuals);
- Changes are to be made to an existing process that involves the processing of personal data;
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data;
  Introducing any new technology that uses or processes personal data in any way.

7 Distribution and Implementation

This document will be made available to all Staff via the CCG internet site. Notification will be sent via regular communications / bulletins arrangements to all staff.A link to this document will be provided from the Information Governance intranet site.

8 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance Team.

The Cyber Assurance and Compliance Manager is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

9 Associated Documentation

This policy should be read in conjunction with:

- Confidentiality and Data Protection Policy
- Information Governance Strategy
- Information Governance Policy and Management Framework
- Freedom of Information Act and Environmental Information Regulations Policy
- Records Management Policy
- Mobile Working Policy
- Network Security Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Anti-Fraud and Bribery Policy
- Whistle Blowing Policy
- Internet and Email Policies and Procedures

10 References

- The Data Protection Act (2018)
- The General Data Protection Regulation
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2012

Policy Consultation Process:

Title of document	Information Security
Author	Abi Dakin
New / Revised document	New – adopted from NHSE
List of persons involved in the consultation process:	Members of the IG/BI/IT Committee

Appendix A Request for Equipment Retention During Long Term Absence

NHS
Leeds
Clinical Commissioning Group

Request for Equipment Retention During Long Term Absences

In exceptional circumstances a member of staff who is expected to be on long term absence (more than 28 days); the manager may request that they retain any equipment that has been provided by the CCG. It is the manager's responsibility to ensure that any equipment is returned on request.

This form should be completed and returned to Leedsccg.gpit@nhs.net.

User Details

Mr/Mrs/Ms/Dr Forename _____ Surname _____

Work Tel _____ Job Title _____

Location Details

Site _____ ie WIRA, Merrion

Department & Team _____

Equipment to be retained:

Laptop Yes ☐ No ☐ Please provide Asset number _____

Mobile Phone Yes ☐ No ☐ Please provide telephone number _____

Monitor Yes ☐ No ☐

Keyboard Yes ☐ No ☐

Mouse Yes ☐ No ☐

Other : _____

NHS
Leeds
Clinical Commissioning Group

Print form and sign by hand or click in box and insert .jpg of signature

Requestor details

Name:

Signed:

Job Title:

Email Address:

Date:

Work Number:

Authorised signatory details (Director/Budget Holder)

Name:

Signed:

Job Title:

Email Address:

Save the file as a PDF before emailing the GPIT inbox