 

# Confidentiality and Security of Information Policy



|  |  |
| --- | --- |
| **Complete the blank cells in the table below. The rest will be added by the corporate team once the policy approved and before it is added to the website.** | |
| **Policy ref no:** | 11 |
| **Responsible Executive Director:** | Deborah El-Sayed |
| **Author and Job Title:** | **Information Governance Team, SCW CSU** |
| **Date Approved:** | 25th November 2024 |
| **Approved by:** | Shane Devlin, Chief Executive |
| **Date of next review:** | November 2026 |

## Policy Review Checklist

|  |  |  |
| --- | --- | --- |
|  | **Yes/No/NA** | **Supporting information** |
| Has an Equality Impact Assessment Screening been completed? | Yes | See appendix |
| Has the review taken account of latest Guidance/Legislation? | Yes |  |
| Has legal advice been sought? | No |  |
| Has HR been consulted? | Yes | Via Corporate Policy Review Group |
| Have training issues been addressed? | Yes | Data Security Awareness training provided through ConsultOD |
| Are there other HR related issues that need to be considered? | No |  |
| Has the policy been reviewed by Staff Partnership Forum? | No |  |
| Are there financial issues and have they been addressed? | No |  |
| What engagement has there been with patients/members of the public in preparing this policy? | N/A |  |
| Are there linked policies and procedures? | Yes | Information Governance Policy suite |
| Has the lead Executive Director approved the policy? | Yes | Via Information Governance Group |
| Which Committees have assured the policy? | Yes | Information Governance Group |
| Has an implementation plan been provided? | Yes | See Appendix |
| How will the policy be shared with | Yes | Intranet |
| Will an audit trail demonstrating receipt of policy by staff be required; how will this be done? | No |  |
| Have Data Protection implications have been considered? | Yes |  |

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Consultation** |
|  |  |  |
| 2.0 | 7th June 2024 | Amendments from ICB to ICB, changes to section on disclosure outside the EEA to state UK, references to faxes removed, removal of confidentiality agreement templates and various cosmetic changes |
| 2.1 | 19th June 2024 | Amendments following review from CPRG, cosmetic changes and the addition of the role of the SIRO. |
| 2.2 | 18th October 2024 | Requirements to add reference to managed services and reference to Directorate leads role following IGG review and approval. |

# Table of contents

[Confidentiality and Security of Information Policy 1](#_bookmark0)

[Policy Review Checklist 2](#_bookmark1)

[Table of contents 4](#_bookmark2)

[Confidentiality and Security of Information Policy 5](#_bookmark3)

1. [Introduction 5](#_bookmark4)
   1. [BNSSG ICB Values 5](#_bookmark5)
2. [Purpose and scope 5](#_bookmark6)
3. [Duties – legal framework for this policy 5](#_bookmark7)
4. [Responsibilities and Accountabilities 6](#_bookmark8)
5. [Definitions/explanations of terms used 8](#_bookmark9)
6. [Safe Haven 9](#_bookmark10)
7. [Processes and Requirements 10](#_bookmark11)
8. [Confidentiality Audits 14](#_bookmark12)
9. [Contracts of Employment 14](#_bookmark13)
10. [Disciplinary 14](#_bookmark14)
11. [Abuse of Privilege 14](#_bookmark15)
12. [Training requirements 14](#_bookmark16)
13. [Equality Impact Assessment 15](#_bookmark17)
14. [Implementation and Monitoring Compliance and Effectiveness 15](#_bookmark18)
15. [Countering Fraud, Bribery and Corruption 15](#_bookmark19)
16. [References, acknowledgements and associated documents 16](#_bookmark20)
17. [Appendices 17](#_bookmark21)
    1. [Equality Impact Assessment 17](#_bookmark22)
    2. [Implementation Plan 17](#_bookmark23)

# Confidentiality and Security of Information Policy

## Introduction

The ICB has a legal obligation to comply with all appropriate legislation in respect of, Confidentiality, Data, Information and Cyber/IT Security. It also has a duty to comply with guidance issued by NHS England, the Information Commissioner’s Office (ICO), Department of Health and other advisory groups to the NHS or professional bodies.

The ICO has the powers to impose fines or other penalties or corrective measures upon the organisation, and/or employees for non-compliance with relevant legislation and national guidance.

This policy is supported with practical guidance for staff provided in the Data Security and Information Governance Staff Handbook.

### BNSSG ICB Values

This policy contributes to the values of the ICB by ensuring that the ICB acts with integrity. It underpins individuals’ right to privacy, ensures that confidential information is protected and facilitating the use and legitimate sharing of information enabling us to work better together.

## Purpose and scope

This Policy details how the ICB will meet its legal obligations and NHS requirements concerning confidentiality, information security standards and will operate such procedures ensuring that confidential information sent to or from the organisation is handled in such a way as to minimise the risk of inappropriate access or disclosure.

This policy applies to all staff and individuals working for or on behalf of the ICB.

For the purposes of this policy, where Personal or Special Categories of Data are described, this will include data that is owed a duty of confidentiality under the Common Law.

## Duties – legal framework for this policy

All staff have a legal duty of confidence to keep confidential data private and secure and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

* Talk openly about confidential matters in public places or where they can be overheard.
* Leave any assets containing personal, commercially confidential or special categories of personal data unattended, this includes telephone messages, computer printouts, faxes and other documents.
* Leave a computer logged on to a system where information can be accessed or viewed by another person without authority to view that information.
* Staff must not use someone else’s password to gain access to data. Action of this kind will be viewed as a violation under the Computer Misuse Act 1990 and a serious breach of the ICBs Acceptable Use Policy. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

## Responsibilities and Accountabilities

#### Chief Executive

The Chief Executive has overall responsibility for the Confidentiality and Security of Information Policy within the ICB. Where there is a significant concern regarding the ability of the ICB to evidence its obligations to handle information confidentially or a breach has occurred the matter will be brought to the attention of the ICB Executive Management Team.

#### Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner for the ICB is the Chief Transformation, Data, and Digital Officer/Chief Digital Information Officer, an executive board member with allocated lead responsibility for the organisation’s information risks and provides the focus for management of information risk at executive management level. The Chief Executive must receive assurances from the SIRO that information risk is being managed suitably and successfully throughout the ICB, and for any services contracted by the organisation. The Caldicott Guardian, the Data Protection Officer, the IG Manager (SCW), and the Information Asset Owners (IAOs) provide support to the SIRO.

#### Caldicott Guardian (CG)

The Caldicott Guardian is a member of the Executive Management Team and a senior health or social care professional with responsibility for promoting clinical governance or equivalent functions and advising on confidentiality issues. The Caldicott Guardian acting as the conscience of the organisation plays a key role in ensuring that the ICB satisfies the highest practical standards for handling patient/staff identifiable information. The Caldicott Guardian serves as part of a broader Caldicott function and is supported by the Data Protection Officer and SCW Information Governance Team.

#### Data Protection Officer (DPO)

The Data Protection Officer (DPO) will report directly to the Governing Body in matters relating to data protection assurance and compliance, without prior oversight by their line manager.

The DPO must ensure that their responsibilities are not influenced in anyway and should a potential conflict of interest arise report this to the highest management level.

The DPOs cannot hold a position within the organisation that can be considered a key decision maker in relation to what personal data is collected and used

The Data Protection Officer (DPO) is the person within the ICB that will ensure that Information Governance incidents which are likely to result in a risk to the rights and freedoms of individuals the ICO (Information Commissioner’s Office) is informed within 72 hours. They are also part of the Data Protection Impact Assessment (DPIA) process.

#### Directorate Information Governance Lead

The Directorate Information Governance Lead role is a senior member of staff who has been identified to represent a ICB Directorate and has responsibility for Directorate compliance to Information Governance processes. This includes being a member of the ICB Information Governance Group and providing support for the requirements of the Data Protection and Security Toolkit.

#### Information Asset Owners (IAO) and Information Asset Administrators (IAA)

The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result, they are able to understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO on the security and use of the assets. The Information Governance Team will support the IAOs in fulfilling their role. Information Asset Administrators are required to support the IAO’s and SIRO who will work with the Information Governance Team to ensure staff apply the data protection legislation and Caldicott Principles within daily working practices.

The ICB Information Governance Management Framework details the hierarchical structure in place that underpins and ensures good governance processes are adhered to within the organisation.

#### SCW Information Governance Service

SCW provides IG support services in line with the information governance service specification under any Service Level Agreement for IG Service.

## Definitions/explanations of terms used

All information relating to Personal Confidential Data (PCD), as defined in the 'Confidentiality: NHS Code of Practice', personal, commercially confidential or special categories of personal data and any information that may be deemed confidential or ‘sensitive’, must be kept secure at all times. The ICB will ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

#### Categories of Data

|  |  |
| --- | --- |
| Personal Data (derived from UK GDPR) | Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online  identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person |
| ‘Special Categories’ of Personal Data (derived from the UK GDPR) | ‘Special Categories’ of Personal Data is different from Personal Data and consists of information relating to:   * The racial or ethnic origin of the data subject * Their political opinions * Their religious beliefs or other beliefs of a similar nature * Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 * Genetic data * Biometric data for the purpose of uniquely identifying a natural person * Their physical or mental health or condition * Their sexual life |
| Personal Confidential Data | Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and  ‘confidential’ includes information ‘given in confidence’ and ‘that which is owed a duty of |

|  |  |
| --- | --- |
|  | confidence’. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013). |
| Commercially confidential Information | Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations. |

## Safe Haven

A ‘Safe Haven’ is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place to ensure that personal data is communicated safely and securely. It is a safeguard for personal data, which enters or leaves the organisation whether this is electronically, fax, post or other means.

All members of staff handling personal data, whether paper based or electronic, must adhere to relevant Safe Haven principles. For example, within Finance there is a Controlled Environment for Finance which must follow agreed processes when handling patient data.

#### Where safe haven procedures should be in place

Safe haven procedures should be in place in any location where large amounts of personal or special categories of personal data is being received, held or communicated especially where the information is of a highly confidential nature.

#### Sending personal or special categories of personal data

Always consider whether it is necessary to share Personal or Special Categories of Personal data and if data minimisation can achieve the desired outcome. Within the NHS, confidential data should always be addressed to the appropriate safe haven within the recipient’s organisation using the appropriate security classification for example:

OFFICIAL – SENSITIVE: COMMERCIAL

Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to ICB or a commercial partner if improperly accessed.

Or

OFFICIAL – SENSITIVE: PERSONAL

Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences

Some NHS organisations may still work to previous guidance; consequently, any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

For specific guidance and procedures in respect of telephony enquiries, e-mails and post, please refer to the IG staff handbook.

## Processes and Requirements

#### Database Management

All databases should form part of an Information Asset Register (IAR). A list of the organisations IAR’s will be maintained by SCW IG Team but remain the responsibility of the individual team Information Asset Owner’s (IAO’s) in the ICB.

For the purposes of this policy the term “Database” refers to a structured collection of records or data held electronically which contains personal or special categories of personal data, which has been provided in confidence or commercially confidential data. In the event that further guidance is needed in respect to what constitutes a database please contact the SCW IG Team [SCWCSU.scwdataprotection-bnssg@nhs.net](mailto:SCWCSU.scwdataprotection-bnssg@nhs.net)

#### IT Back Ups

SCW IT Services Teams are responsible for ensuring that appropriate back up procedures are available and implemented.

#### Disclosure of Information & Information Flows

It is important that information that identifies individuals (such as the general public, patients and/or staff) should only be shared on a strict need to know basis and with the appropriate authorisation. Strict controls governing the disclosure of identifiable information is a requirement of the Caldicott recommendations [The Caldicott Principles - GOV.UK](https://www.gov.uk/government/publications/the-caldicott-principles) [(www.gov.uk)](https://www.gov.uk/government/publications/the-caldicott-principles)

All disclosures or flows of data, either electronically or in hard copy, which contain personal, special categories of personal data, or commercially confidential information and indeed any information that may be deemed confidential or ‘sensitive’ must be included in the relevant Information Asset Register and Data Flow Mapping tool.

If any personal, commercially confidential or special categories of personal data need to be shared electronically via removable media devices (such as encrypted disc, encrypted USB memory stick etc.) or manually (for hard copy records) via courier or postal service, a Data Protection Impact Assessment (DPIA) should be considered and carried out where the security and confidentiality of this information is potentially at risk. For further guidance or advice please contact the SCW IG Team [SCWCSU.scwdataprotection-bnssg@nhs.net](mailto:SCWcsu.scwdataprotection-bnssg@nhs.net)

Contracts between the ICB and third parties with whom information is shared must include Data Protection and Confidentiality clauses.

The ICB is a ‘Controller’ either solely or jointly, as defined in the UK General Data Protection Regulation (UK GDPR) and uses ‘Processors’ or ‘sub Processors’. All of whom are obliged to meet the requirements of the Data Protection Legislation and must be correctly identified in contracts and agreements with standard checks of evidence of compliance undertaken prior to contract terms being signed. Processors must only act in accordance with directions from the identified Controller.

Where the ICB commissions providers to provide clinical services the relationship is different, the provider will normally be a Controller in their own right.

#### Disclosure of Information outside the United Kingdom

No personal, commercially confidential or special categories of personal data should be disclosed or transferred outside of the UK to a country or territory which does not ensure an adequate level of protection.

In the event that there is a need to process information outside of the UK, the Data Protection Officer must be consulted prior to any agreement to transfer or process the information.

#### The Legal Basis for sharing personal, commercially confidential or special categories of personal data

To ensure that data is shared appropriately, care must be taken to check that a clear basis in law is established that permits or obligates the sharing. The completion of a DPIA is a statutory requirement when considering new processing including the sharing of Special Categories of personal data as defined in the UK GDPR.

It is important to consider how much data is required and ensure that the minimal amount necessary is disclosed.

Data can normally be disclosed when effectively anonymised/pseudonymised in line with legislative requirements and the ICO Anonymisation Code of Practice [anonymisation-](https://ico.org.uk/media/1061/anonymisation-code.pdf) [code.pdf (ico.org.uk)](https://ico.org.uk/media/1061/anonymisation-code.pdf), unless subject to other restrictions e.g. NHS Digital contracts.

When the information is required by law or under a court order in situations such as the detection and prevention of serious crime, staff should discuss the matter with the SCW Information Governance Consultant or the Data Protection Officer. [SCWCSU.scwdataprotection-bnssg@nhs.net](mailto:SCWcsu.scwdataprotection-bnssg@nhs.net)

Data can be disclosed in identifiable form, with the individual’s explicit consent or the appropriate lawful basis under the UK GDPR or with support from NHS England who will apply for the necessary approval from the appropriate authority for example, the Confidentiality Advisory Group (CAG).

In potential safeguarding situations where it is decided that information should be shared according to the duties placed on the organisation to protect vulnerable people, staff should contact their line manager and if necessary, discuss with the Data Protection Officer, who will provide advice and guidance and in cases where a decision to share is not clear. Where necessary it may be prudent to inform and obtain approval of the Caldicott Guardian for the disclosure [SCWCSU.scwdataprotection-bnssg@nhs.net](mailto:SCWCSU.scwdataprotection-bnssg@nhs.net)

When necessary and agreed as part of the DPIA process, a Data Sharing or Data Processing Agreement must be completed before any data is transferred. The various agreements will set out any conditions for use and identify the secure method of transfer. For further information on Agreements contact the SCW IG Team [SCWCSU.scwdataprotection-](mailto:SCWCSU.scwdataprotection-bnssg@nhs.net) [bnssg@nhs.net](mailto:SCWCSU.scwdataprotection-bnssg@nhs.net)

There are Acts of Parliament, listed below (not exhaustive), which govern the disclosure of personal and special categories of personal data. Some of these Acts make it a legal requirement to disclose and others state that information cannot be disclosed.

* Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
* Education Act 1944 (for immunisations and vaccinations to NHS Public Health England from schools)
* Births and Deaths Act 1984
* Police and Criminal Evidence Act 1984
* Human Fertilisation and Embryology (Disclosure of Information) Act 1992
* Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
* Abortion Act 1967
* The Adoption Act 1976
* Children Act 2004

In the event that a request for disclosure is made referencing any of these Acts appropriate advice and support should be sought and the Data Protection Officer to advise [bnssg.data.protection@nhs.net](mailto:bnssg.data.protection@nhs.net)

#### Secure methods of Sharing Information

Care must be taken when transferring data to ensure that the method used is encrypted where necessary and is always secure. Staff must ensure that appropriate standards and safeguards are in place in respect of telephony enquiries, e-mails and post.

It is policy that emails containing any personal, commercially confidential or special categories of personal data should be sent using an NHS.net account. Therefore, staff emailing from @nhs.net accounts to another @nhs.net account, can be confident that the content of the message is encrypted and secure.

In circumstances where the receiving organisation does not hold a NHS.net account, the Encryption Guide for NHSmail must be followed to ensure all personal, commercially

confidential or special categories of personal data sent outside of NHSmail is protected [Guidance for sending secure email (including to patients) - NHS England Digital](https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email)

The service dictates you must use [secure] in square brackets in the subject line of your email. An encrypted email sent from an NHSmail address (ending @nhs.net) will contain a link to access the encrypted message.

Staff must ensure they use the NHSmail platform in accordance to the published guidance, policies and procedures to ensure appropriate and secure usage NHS mail guidance.

Care must be taken to ensure confidential information is not entered in the subject header when sending an email. Please seek advice from SCW IG Team if required.

If information is required to be sent to a member of the public, using their non-secure email address, it is the responsibility of the member of staff to ensure that the member of public is provided with a clear explanation of the risks of using unsecure email addresses and records of this conversation should be kept.

#### Mobile and remote working

Special care will need to be taken by staff when working remotely to ensure the security of both information and hardware. Staff may need to carry organisational data and assets with them which could be or contain personal, commercially confidential or special categories of personal data e.g. on an encrypted laptop, encrypted USB stick or as paper documents. When working away from ICB locations, staff must ensure that their working practices comply with the ICB policies listed below. Any removable media must be encrypted as per the NHS Encryption Guidance Standards.

Staff must not leave personal, commercially confidential or special categories of personal data unattended at any time and ensure that it is kept in a secure lockable place when working remotely.

Staff must minimise the amount of physical personal, commercially confidential or special categories of personal data that is taken away from ICB premises.

When in transit staff must ensure that any personal, commercially confidential or special categories of personal data is transported in a secure manner, is kept out of sight whilst being transported (i.e. the boot of a car) and removed to a more secure location on arrival at their destination. Do not leave equipment or assets in a car.

Staff are responsible for ensuring that any data or assets taken home are kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have access to the data.

Staff must not forward any personal, commercially confidential or special categories of personal data via email to their home email account or store the data on a privately owned

computer, storage device or other technology such as a cloud storage solution that is not provided by the ICB.

## Confidentiality Audits

Good practice requires that all organisations that handle personal, commercially confidential or special categories of personal data put in place processes to highlight actual or potential breaches of security or confidentiality in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by SCW Information Governance Team through a programme of audits. Confidentiality Audits will be undertaken at least annually and reported to the Information Governance Group.

## Contracts of Employment

Staff contracts of employment are produced and supported by SCW Human Resources (HR) department. All contracts of employment include a clause on adherence to the data protection legislation and the common law duty of confidentiality. Agency, Contractors and any other non-contract staff (off payroll workers) working on behalf of the ICB are subject to the same rules which will be enforced and recorded through the use of confidentiality agreements.

All employees will be made aware of their responsibilities through their Statement of Terms and Conditions, their information governance training, staff induction and all relevant policies, procedures and guidance.

## Disciplinary

A breach of the Data Protection Legislation requirements could result in a member of staff facing disciplinary action.

## Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any data relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and the Data Protection Legislation.

## Training requirements

#### Information Asset Owner and Information Asset Administrators

The SCW IG Team provides training for Information Asset Owners and Administrators through use of a workbook or face to face sessions. Training will cover an overview and Data Protection requirements, the IG Structures within the ICB, the role of Information Asset Owners and Administrators and practical advice on fulfilling their role.

#### 12.2. All Staff

All new starters to the ICB inclusive of temporary, bank staff and contractors must undertake Data Security Awareness training via the ConsultOD portal, to evidence compliance with the

Data Protection Legislation and the DSP Toolkit assertions as part of the induction process. Extra training will be given to those dealing with formal requests for access to personal information. A register will be maintained of all staff who have completed the online training and those who have attended face to face training sessions where these are offered. Annual Data Security and Awareness training should be undertaken by all staff via the ConsultOD portal.

All staff will be provided with a copy of the Data Security and Information Governance Handbook which includes details of how to manage personal information and report incidents via ConsultOD. All staff are expected to download and read the handbook annually.

## Equality Impact Assessment

See attached.

## Implementation and Monitoring Compliance and Effectiveness

This Policy will be reviewed every two years or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from NHS England, NHS Digital and the Information Commissioner or any relevant case law.

This policy will be monitored by the SCW IG Team to ensure any legislative changes that occur before the review date are incorporated.

## Countering Fraud, Bribery and Corruption

The ICB is committed to reducing and preventing fraud, bribery and corruption in the NHS and ensuring that funds stolen by these means are put back into patient care. During the development of this policy document, we have given consideration to how fraud, bribery or corruption may occur in this area. We have ensured that our processes will assist in preventing, detecting and deterring fraud, bribery and corruption and considered what our responses to allegation of incidents of any such acts would be.

In the event that fraud, bribery or corruption is reasonably suspected, and in accordance with the Local Counter Fraud, Bribery and Corruption Policy, the ICB Team will refer the matter to the ICB’s Local Counter Fraud Specialist for investigation and reserve the right to prosecute where fraud, bribery or corruption is suspected to have taken place. In cases involving any type of loss (financial or other), the ICB will take action to recover those losses by working with law enforcement agencies and investigators in both criminal and/or civil courts.

1. References, acknowledgements and associated documents For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. The legislation listed below also refers to issues of security of personal confidential data.

* UK General Data Protection Regulations
* Data Protection Act 2018
* Access to Health Records 1990
* Access to Medical Reports Act 1988
* Human Rights Act 1998
* Freedom of Information Act 2000
* Regulation of Investigatory Powers Act 2000
* Crime and Disorder Act 1998
* Computer Misuse Act 1990
* Criminal Justice and Immigration Act 2008
* Health and Social Care Act 2012
* Health and Social Care (Safety and Quality) Act 2015
* The Privacy and Electronic Communications (EC Directive) Regulations 2003
* Fraud Act 2006

The following are the main publications referring to security and or confidentiality of personal confidential data:

* Confidentiality: NHS Code of Practice
* CQC Code of Practice on Confidential Personal Information
* NHS England: A Guide to Confidentiality in Health and Social Care
* NHS England Confidentiality Policy
* Records Management Code of Practice for Health and Social Care Information Security: NHS Code of Practice
* Employee Code of Practice (Information Commissioner)
* Caldicott Report.

This Policy should be read in conjunction with other Information Governance (IG) Policies including:

* Information Governance Framework
* Information Governance Policy
* Records Management Policy
* Confidentiality and Security of Information Policy
* Individual Rights Policy
* Disciplinary Policy
* Data Security and Information Governance Handbook
* IT Acceptable User Policy

## Appendices

### Equality Impact Assessment



EHIA for C&IS Policy.pdf

### Implementation Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Target Group** | **Implementation or Training objective** | **Method** | **Lead** | **Target start date** | **Target End date** | **Resources Required** |
| IAO/IA A | To ensure  knowledge of Policy and content | IAO/IAA meeting | AG | Dec 2024 | Dec 2024 | None |
| All staff | To ensure awareness of  Policy | The Voice | AG | Dec 2024 | Dec 2024 | None |
| All staff | To ensure access to Policy is  available | The Hub | AG | Dec 2024 | Dec 2024 | None |