NHS
Cornwall and Isles of Scilly

Confidentiality Code of Conduct for Employees

Date approved: 11 April 2025

This policy may not be suitable for users of assistive technology. If you use assistive technology (such as a screen reader) and need a version of this document in a more accessible format, please email CIOSicb.corporategovernance@nhs.net. Please tell us what format you need. It will help us if you say what assistive technology you use.

Document control sheet

Title of document:	Confidentiality Code of Conduct for Employees
Originating Directorate:	Corporate Governance
Originating team:	Information Governance
Document type:	Protocols
Subject category:	Information Governance
Author(s) name:	Bev Gallagher and Jodeigh Phelps
Date ratified:	11 April 2025
Ratified by:	Information Governance Steering Group
Review frequency:	Two years
To be reviewed by date:	11 April 2027
Target audience:	All employees, bank or agency staff, locums, student placements, GB Members, mandated GPs, clinical leads, contractors and individuals/volunteers supporting NHS CIOS ICB in its operational duties
Can this policy be released under FOI?	Yes
	Give reasons for exemption if no:

Version control

Version No	Revision date	Revision by	Nature of revisions
V1.0	February 2016	Bev Gallagher	General amendments and updates to content.
V1.0	November 2018	Jodeigh Phelps	Updated for new policy template; changes to legislation, i.e. GDPR and DPA 2018; roles and responsibilities; plus DPIA requirements
V2.0	February 2019	Jodeigh Phelps	Updates following feedback from staff. Revise terminology relating to Gillick competence; add in information regarding secure storage and social media. EIA added.
V2.1	February 2025	Milton Shoriwa/Mike Cottam (SCW CSU)	Formal IG review and updates - general

NHS
Cornwall and
Isles of Scilly

Contents

Contents 4
1. Introduction 5
2. Purpose 5
3. Key definitions 7
4. Responsibilities 8
5. Confidential information 10
6. Requests for information on individuals and individual consent 12
7. Telephone enquiries 15
8. Requests for information by the police, legal firms and the media 16
9. Disclosure of information to other employees of NHS CIOS ICB 17
10. Abuse of privilege 18
11. Carelessness 19
12. Use of internal and external post 20
13. Faxing 21
14. Storage of confidential information 21
15. Disposal of confidential information 22
16. Confidentiality of passwords, PIN numbers, smartcards 22
17. Emailing confidential information 23
18. Instant messaging services 24
19. Social Media 24
20. Working at home 25
21. Copying of software 25
22. Compliance and Monitoring 26
23. Monitoring 26
24. Update and review 26
25. Appendix 1: Regulatory Framework 27
26. Appendix 2: NHS CIOS Related Policy Documents 29
27. Appendix 3: Equality Impact Assessment 30

1. Introduction

1.1. The Code of Conduct for Staff serves as a supportive guide to ensure that all employees of NHS Cornwall and Isles of Scilly Integrated Care Board (NHS CIOS ICB) understand their responsibilities regarding confidentiality, data protection, and information governance.

1.2. This Code provides:

- Clear guidance on confidentiality responsibilities, covering both personally identifiable information (PII) and confidential corporate information.
- Detailed instructions on the use and disclosure of personally identifiable information, ensuring compliance with UK GDPR, the Data Protection Act 2018, and the Common Law Duty of Confidentiality.
- Guidance on obtaining consent when using personal information for purposes beyond direct care, in line with the Caldicott Principles.
- Support for respecting patient, public, and staff choices regarding how their information is used and shared.
- Information on conducting Data Protection Impact Assessments (DPIAs) to identify and mitigate risks when processing personal data.
- A framework for demonstrating due diligence and good governance in managing NHS CIOS ICB's information assets, ensuring compliance with national and local policies.

1.3. All staff must familiarise themselves with this Code and apply it in their daily work to uphold the highest standards of confidentiality, trust, and data security.

2. Purpose

2.1. Legal Duty of Confidentiality

All employees working in or with the NHS are bound by a legal duty of confidence to protect personal information encountered in the course of their work. This duty is not only a requirement of contractual responsibilities but also a legal obligation under:

- The Data Protection Act 2018 (DPA 2018)
- The Common Law Duty of Confidentiality
- The UK General Data Protection Regulation (UK GDPR)

2.2. Professional and Ethical Responsibilities

In addition to legal requirements, health and care professionals must adhere to the Code(s) of Conduct set by their respective professional bodies, such as:

- General Medical Council (GMC)
- Nursing and Midwifery Council (NMC)
- Health and Care Professions Council (HCPC)
- Code of Conduct for NHS Managers

This Code also reflects the rights and pledges of the NHS Constitution, ensuring that NHS values and principles are upheld.

2.3. Confidentiality of Personal and Corporate Information

Employees are obliged to keep all personal identifiable information strictly confidential, including:

- Patient and public records
- Employee records
- Employees may also come into contact with non-person identifiable but sensitive information, such as:
- Business and financial information ("in confidence")
- Corporate documents, contracts, and procurement records

These must be treated with the same level of care as personal data.

2.4. Rules on Disclosure and Information Sharing

Disclosure and sharing of personal identifiable information must comply with the Data Protection Act 2018 and UK GDPR.

Confidential corporate information is subject to other legal and regulatory requirements, such as the Freedom of Information Act 2000 and contractual obligations.

2.5. Accountability for Confidentiality Breaches

The core principle of this Code of Conduct is that no employee shall:

- Breach their legal duty of confidentiality.
- Enable or allow others to breach confidentiality.
- Attempt to bypass or compromise NHS CIOS ICB's security systems and controls.

2.6. Protecting Staff Through Awareness

This Code has been developed to protect staff by ensuring they are aware of correct procedures and do not inadvertently breach:

- Legal requirements

- Organisational policies and procedures
- NHS Codes of Practice

2.7. **The Caldicott Principles**

In addition to data protection laws, all employees must adhere to the Caldicott Principles, which apply to the handling of confidential patient information:

- Justify the purpose for using confidential information.
- Only use confidential information when absolutely necessary.
- Use the minimum amount of information required.
- Access must be limited to those who need to know.
- Everyone must understand their responsibility to protect information.
- Ensure compliance with the law and best practice.
- Recognise that the duty to share information can be as important as the duty to protect patient confidentiality.

All staff must follow the eight Caldicott Principles, particularly the fundamental requirement that personal confidential data must only be used when absolutely necessary and shared on a need-to-know basis with the minimum necessary information disclosed. Failure to uphold these principles could result in disciplinary action, regulatory scrutiny, or legal consequences.

3. Key definitions

3.1. **DPA 2018 (Data Protection Act 2018)** – The UK legislation that supplements and enforces the UK General Data Protection Regulation (UK GDPR). It sets out specific provisions for data protection and privacy, including exemptions and legal bases for processing personal data.

3.2. **DPIA (Data Protection Impact Assessment)** – A risk assessment that must be conducted for all new or significantly changed processing of personal information to ensure compliance with data protection laws and mitigate potential risks to individuals' privacy.

3.3. **UK GDPR (UK General Data Protection Regulation)** – The post-Brexit UK version of GDPR, based on the original European General Data Protection Regulation (GDPR), which came into effect in May 2018. It governs how organisations handle personal data, ensuring transparency, accountability, and data security.

3.4. **Record** – Any information held by NHS CIOS ICB that meets the definition of a health or corporate record, including:

- Health records (e.g., patient medical notes, treatment records)
- Personal records (e.g., information on the relatives of patients, service users, or members of the public)
- Employee records (e.g., HR files, employment history)
- Corporate records (e.g., meeting minutes, contracts, procurement documents, invoices, and financial accounts)

3.5. **Staff** – This definition applies broadly to all individuals working for or on behalf of NHS CIOS ICB, including:

- Permanent employees
- Bank or agency staff
- Locums
- Student placements and trainees
- Mandated GPs and clinical leads
- Contractors and third-party service providers
- Volunteers or individuals supporting ICB operations

4. Responsibilities

4.1. Confidentiality is the responsibility of all employees of NHS CIOS Integrated Care Board (ICB). All staff have a legal, professional, and ethical duty to protect personal and sensitive information, ensuring it is handled securely and used appropriately. This duty aligns with:

- UK General Data Protection Regulation (UK GDPR) – governing the processing and protection of personal data.
- Data Protection Act 2018 – outlining specific UK data protection provisions.
- The Caldicott Principles, which emphasise the need to safeguard patient confidentiality while enabling appropriate information sharing for care
- The Common Law Duty of Confidentiality – requiring personal information to be kept confidential unless there is a legal basis to disclose it.
- The Human Rights Act 1998 (Article 8: Right to Privacy) – ensuring individuals' rights to privacy and family life.

- Freedom of Information Act 2000 – regulating public access to non-personal information.
- NHS England's Records Management Code of Practice
- NHS CIOS ICB's Information Governance policies.

4.2. This Code should be alongside the NHS CIOS ICB's local policies and procedures for confidentiality, information governance, and data protection—these are listed in Appendix 2.

4.3. Staff must ensure they are familiar with these related policies and apply them in their daily work to maintain high standards of confidentiality and data security.

4.4. **Data Protection Officer (DPO)**

The DPO plays a key role in ensuring confidentiality is upheld by:

- Monitoring compliance with data protection laws and NHS confidentiality standards.
- Advising on data protection obligations and best practices for securing personal information.
- Overseeing Data Protection Impact Assessments (DPIAs) to identify and mitigate risks to confidentiality.
- Acting as the primary contact for data subjects and the Information Commissioner's Office (ICO) regarding privacy concerns.

4.5. **Senior Information Risk Owner (SIRO)**

The SIRO is responsible for:

- Embedding a culture of confidentiality and data security across the organisation.
- Managing information risks and ensuring robust controls are in place to prevent data breaches.
- Providing assurance to the Governing Body that patient and staff information is handled securely and in accordance with NHS policies.

4.6. **Caldicott Guardian**

The Caldicott Guardian, usually the Chief Medical Officer, ensures that confidentiality remains a top priority by:

- Overseeing the use and sharing of confidential patient and service user information.

- Ensuring compliance with the Caldicott Principles, which require a justified purpose for using patient data and that the least amount of identifiable data is used wherever possible.
- Supporting staff in making informed choices about handling personal data while maintaining privacy and trust.

For more detailed information on confidentiality responsibilities, please refer to NHS CIOS ICB's Information Governance Strategy.

5. Confidential information

5.1. Confidential information includes any data that relates to patients, staff, their family, or friends, in any format. It also covers confidential corporate information belonging to NHS CIOS Integrated Care Board (ICB).

5.2. **Formats of Confidential Information**

5.2.1. Confidential information may be stored or recorded in various formats, including but not limited to:

- Paper records (e.g. medical notes, audits, meeting minutes, procurement records)
- Electronic files (e.g. databases, emails, scanned documents)
- Portable devices (e.g. laptops, tablets, mobile phones, USB sticks, digital cameras)
- Removable media (e.g. CDs, memory sticks)
- Visual and audio formats (e.g. videos, photographs, voicemail recordings)
- Verbal communications (e.g. discussions overheard in public areas)

5.2.2. Staff must ensure that confidential information is protected, regardless of the format in which it is stored or transmitted.

5.3. **Person Identifiable Information (PII)**

5.3.1. Person Identifiable Information (PII) is any data that can identify an individual, either directly or indirectly. Examples include:

- Full name
- Address or postcode
- Date of birth
- NHS number
- National Insurance number

- Visual identifiers (e.g. photographs, CCTV footage)

5.3.2. Even a combination of non-specific details (e.g. date of birth + postcode) may be sufficient to identify an individual.

5.3.3. For more guidance on identifiable information, visit the Information Commissioner's Office (ICO) website.

5.4. **Special Category Data**

5.4.1. Under UK GDPR, certain types of data are classified as Special Category Data, as they require enhanced protection due to their sensitivity. These include:

- Race or ethnic origin
- Political or philosophical beliefs
- Religious beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Health data
- Sex life or sexual orientation

5.5. **Risks of Processing Special Category Data**

5.5.1. Because Special Category Data is highly sensitive, it poses a greater risk to individuals' rights and freedoms, such as:

- Increased risk of unlawful discrimination
- Potential misuse of medical or genetic information
- Exposure of political or religious beliefs

5.5.2. For this reason, additional legal safeguards must be in place before processing such data.

5.6. Highly Sensitive Information

5.6.1. Certain types of information are subject to specific legal protections and can only be processed under strict conditions. Examples include:

- In-vitro fertilisation (IVF) records
- Sexually transmitted disease (STD) diagnoses
- Adoption records

- Gender reassignment information
- HIV status
- Termination of pregnancy records

5.6.2. Only organisations that meet the legal requirements under UK GDPR can process these categories of information.

5.6.3. Staff requiring further guidance should contact the Corporate Governance team at: ciosicb.corporategovernance@nhs.net

5.7. **Confidentiality After Death**

5.7.1. There are no specific legal obligations under UK GDPR regarding confidentiality of the deceased.

5.7.2. However, the Department of Health and the General Medical Council (GMC) recognise an ethical duty to maintain confidentiality after death.

5.7.3. Relatives of the deceased have a right to expect continued privacy and respect regarding their loved one's information.

5.7.4. Certain legislation, such as the Access to Health Records Act 1990, governs access to deceased patients' medical records under specific conditions.

5.7.5. All staff must ensure that the confidentiality of deceased patients is handled sensitively and ethically.

6. Requests for information on individuals and individual consent

6.1. NHS CIOS ICB employees must never disclose identifiable information without a clearly identified legal obligation. All requests for identifiable information must be:

- Based on a justified need.
- Assessed for legal compliance.
- Approved by the Caldicott Guardian, SIRO, Data Protection Officer (DPO), or Head of Information Governance (IG), where necessary.

6.2. **Consent for Disclosure**

6.2.1. Written consent from the individual may be required before disclosure.

6.2.2. If the individual cannot give consent, consult with the most appropriate person, such as:

- The health professional in charge of care.
- A family member (if legally authorised).
- The employee's line manager (for staff information).

6.2.3. Each case should be assessed individually based on the situation and legal requirements.

6.3. **Legal Basis for Consent Under Data Protection Laws**

6.3.1. Under UK GDPR and the Data Protection Act 2018, implied consent for processing personal data is no longer sufficient. The individual must:

- Explicitly opt-in to consent.
- Be provided with clear information on how their data will be used.
- Have their recorded consent available for inspection.

6.4. **Consent for Direct Healthcare**

6.4.1. For direct healthcare purposes, consent is not always required, as the legal basis for processing may be:

- Legitimate interest
- Public task
- Vital interest

6.5. **Consent for Non-Care Purposes**

6.5.1. In most cases, explicit consent is required for sharing identifiable information for non-care purposes, except in circumstances where disclosure is:

- Required by law (e.g., to the courts).
- In the public interest (e.g., safeguarding concerns).
- Requested by the police or government departments (subject to legal justification).

6.6. **Confidentiality and Trust**

6.6.1. Individuals have a right to expect that:

- Their personal information will be held securely and confidentially.
- Information will remain accurate and available when needed.
- NHS staff will maintain trust and transparency in handling their data.

6.6.2. If asked to provide patient, individual, or staff information, you must:

- Ensure the individual is aware of disclosures made for care purposes or clinical audits.

- Use the "How We Use Your Information" leaflet in discussions about information sharing.
- Ensure accessibility (e.g., alternative formats/languages) by referring individuals to the Engagement Team.
- Obtain explicit consent before sharing identifiable data for non-care purposes.
- Forward Subject Access Requests (SARs) to the Corporate Governance Team in accordance with the ICB's Information Rights Policy.
- Seek HR advice before releasing employee personal data.
- Obtain appropriate approval before sharing confidential corporate information beyond authorised circulation lists.

6.7. **Disclosures Without Consent**

6.7.1. If information must be disclosed outside the direct care team and the patient, client, or employee has not given consent, or has refused consent, you may only disclose information if:

- It is justified in the public interest, such as preventing serious harm to the individual or others.
- There is a legal obligation or court order requiring disclosure.

6.8. **Safeguarding and Child Protection**

6.8.1. For child protection concerns, follow national and local safeguarding policies.

6.8.2. Under the Data Protection Act 2018, the age of consent for processing personal data is 13 years. If you have concerns about disclosing information about a child, contact the Safeguarding Team for guidance.

6.9. **Purpose Limitation**

6.10. NHS CIOS ICB follows the principle that:

- Information given for one purpose must not be used for another purpose without the individual's explicit consent.
- This is a fundamental requirement under UK GDPR and the Data Protection Act 2018.

6.11. **Right to Restrict Disclosure**

6.11.1. Individuals have the right to restrict the disclosure of their personal information.

6.11.2. Staff must respect this right—no one can override an individual's decision unless:

- The individual is a child (under 13) or lacks capacity, in which case a parent, legal guardian, or someone with mental health decision-making authority may make the decision.
- A legal or safeguarding exception applies.

6.12. **Information Sharing for Individuals Lacking Capacity**

6.12.1. Before sharing personal data about someone who lacks capacity, consider:

- if the requestor legally authorised to act on behalf of the individual?
- Is disclosure in the individual's best interests?
- Can less data be shared to achieve the same purpose?

6.13. **Right to Change Consent Decisions**

6.13.1. Individuals have the right to:

- Change their mind about information sharing at any time before disclosure.
- Withdraw consent to prevent future disclosures for recurring data-sharing activities.

For more information on individuals' eight data rights, refer to the ICB's Data Protection Policy.

6.14. **Handling Concerns About Disclosing Information**

6.14.1. If you have concerns about sharing information, you must:

- Discuss the issue with your line manager.
- If your manager is unavailable, contact the Caldicott Guardian, Head of IG, or the DPO.
- Do not disclose information until the request is properly assessed.

6.14.2. Ensure identity verification before disclosing personal data to third parties.

6.14.3. If you cannot find an appropriate person to advise, record the requestor's details and respond once guidance has been obtained.

7. Telephone enquiries

7.1. Verifying Caller Identity and Entitlement - If a request for information is made over the telephone:

- Always verify the caller's identity before disclosing any information.

- Confirm whether they are legally entitled to receive the requested information.
- If unsure, do not disclose information immediately— instead:
- Take their name, organisation, and contact details.
- Verify their identity independently (e.g., check internal records, official email, or website).
- Call them back using an official contact number rather than the number they provide.

7.2. **Confidentiality of Caller Information**

7.2.1. Even confirming that an individual is known to the organisation or is a staff member may be considered confidential information.

7.2.2. If you are unsure whether to disclose information, do not provide any details until you have:

- Consulted your line manager, the Data Protection Officer (DPO), or the Head of Information Governance (IG).
- Confirmed that disclosure is lawful and appropriate.

7.2.3. Never assume a caller's identity based on familiarity or authority—always verify.

8. Requests for information by the police, legal firms and the media

8.1. Requests from the Police or Legal Firms

8.2. All requests for information from the police or legal firms must be referred to:

- The Data Protection Officer (DPO)
- The Head of Information Governance (IG)
- The Caldicott Guardian

8.3. Do not disclose any information without prior authorisation.

8.4. The requestor must provide a legal basis for the disclosure, such as:

- A court order
- A Data Protection Act 2018 exemption (e.g., crime prevention)
- Schedule 2, Part 1, Paragraph 2 of the Data Protection Act 2018 (allowing disclosure to the police for crime detection/prevention).

8.5. Handling Media Requests

8.5.1. Under no circumstances should you provide any information to the media.

8.5.2. Only the following are authorised to handle media enquiries:

- The Chief Officer responsible for communications
- The Communications Team
- Senior managers following national confidentiality guidance

8.5.3. If you receive any media request (via phone, email, or in person):

- Do not confirm or deny any information.
- Refer the request immediately to the Communications Team.

8.6. **Contacting the Communications Team**

- Email media enquiries to: ciosicb.mediarelations@nhs.net
- For urgent media enquiries outside office hours, call: 01208 251300 and request the on-call director.

8.7. **Verifying Media Requests**

8.7.1. The media may not always disclose their identity or intent upfront.

8.7.2. If you suspect a caller or visitor is from the media, but they do not identify themselves, refer them to the Communications Team for verification.

8.7.3. If you have any doubts about a caller's legitimacy, do not provide any information and contact the Communications Team for guidance.

9. Disclosure of information to other employees of NHS CIOS ICB

9.1. Information about individuals must only be shared on a strict need-to-know basis.

9.2. This applies to all personal and confidential information about patients, staff, and corporate matters.

9.3. If a staff member does not need the information for their role, it must not be disclosed to them.

9.4. Confidential information must be stored securely to prevent unauthorised access or disclosure.

9.5. Digital records should be password-protected and access-controlled.

9.6. Physical records should be stored in locked cabinets or secure areas.

9.7. **Verifying Employee Identity**

- Before sharing any information, confirm the requester's identity:

- Check their NHS ID badge.
- Verify their internal extension number or official email address.

9.8. Where possible, confirm whether the requester is entitled to access the information.

9.9. Just because someone works for the NHS does not mean they are automatically entitled to all information.

9.10. Do not be pressured or bullied into providing information.

9.11. If you feel uncomfortable, refuse the request and escalate it.

9.12. Any concerns about inappropriate requests should be reported to your line manager or the IG/DPO team.

9.13. **Limit the Information You Share**

- Only provide the minimum information necessary to fulfil the request.
- Avoid sharing excessive or irrelevant details.
- If partial information is sufficient, do not disclose full records.

9.14. **Seek Guidance** - If in doubt, do not disclose information. Instead, seek advice from:

- The Head of Information Governance (IG)
- The Data Protection Officer (DPO)
- The Head of HR (for employee-related requests)

10. Abuse of privilege

10.1. Employees must never access or view information relating to:

- Their own records.
- Family members, friends, or acquaintances.
- Any individual where there is no legitimate work-related reason to do so.

10.2. Accessing such information without authorisation is a serious breach of confidentiality and may result in disciplinary action, up to and including dismissal, regulatory investigation by the Information Commissioner's Office (ICO) or potential legal consequences under the Data Protection Act 2018 and UK GDPR.

10.3. If you have any concerns about access to confidential information, speak to your line manager immediately.

10.4. If you suspect a breach of confidentiality by another employee, report it to:

- The Head of Information Governance (IG)
- The Data Protection Officer (DPO)
- The HR Team

11. Carelessness

11.1. Confidentiality breaches can occur accidentally due to carelessness. To prevent this, all staff must follow these best practices:

11.2. Do not discuss sensitive matters—whether about patients, staff, or corporate information—in public places or areas where you may be overheard. This includes:

- Public transport,
- cafes,
- corridors,
- lifts, and reception areas.

11.3. Consider whether it is appropriate to hold discussions in such spaces.

11.4. Employment-related discussions must be held in private, away from other colleagues.

11.5. Never leave health records or confidential documents unattended.

11.6. Store all physical records in locked cabinets when not in use.

11.7. Do not leave confidential paperwork on desks, printers, or communal areas.

11.8. Protect Computer Screens and Digital Displays

- Ensure screens and digital displays are not visible to unauthorised persons.
- Position screens away from public areas.
- If working in a public-facing role, request a privacy screen filter from your line manager.
- Log off or lock your screen when leaving your workstation.
- Lock Your Computer When Unattended
- Always lock your computer screen when stepping away, using: Ctrl + Alt + Delete → Lock or Windows key + L

11.9. Secure Portable Devices and Data

- Store portable devices securely when not in use.
- Lock laptops, USB drives, and other storage devices in a secure drawer or cabinet.
- Do not leave devices unattended in public or shared areas.

11.10. Use Only Authorised NHS Equipment

- Never download, store, or process confidential information on personal laptops, tablets, or phones and Non-NHS CIOS ICB authorised devices.

11.10.2. If remote working, always use NHS-approved and encrypted devices.

11.11. Password Security

- Never share your passwords with anyone—regardless of their seniority.
- Use strong passwords and update them regularly.
- If you suspect your password has been compromised, change it immediately and inform IT security.

12. Use of internal and external post

12.1. Best practice for maintaining confidentiality requires that all correspondence containing personal information is always addressed to a named recipient. Personal data must be addressed to a specific person, a post holder, or a designated safe haven, but never to a generic department, unit, or organisation.

12.2. In cases where mail is intended for a team, it should be addressed to an agreed post holder or team leader. All such mail must be clearly marked as confidential.

12.3. If you receive external correspondence that does not follow this standard, especially if it contains personal data, you must report it immediately to the Corporate Governance team via email: ciosicb.corporategovernance@nhs.net.

12.4. Internal mail containing confidential data must only be sent in a securely sealed envelope, clearly marked ‘Confidential’ or ‘Addressee Only’. Upon delivery, only the named recipient may open the envelope unless specific authorisation has been granted to another individual.

12.5. External mail must also adhere to these confidentiality requirements. Special care must be taken when sending bulk personal information, such as case notes or patient records on paper, disc, or other media. These must be sent via recorded delivery or an NHS courier service to ensure they are only accessed by authorised recipients.

12.6. In some cases, it is advisable to obtain a receipt as proof of delivery, for example, when sending person-identifiable information to a solicitor.

12.7. Person-identifiable notes and other bulky materials must only be transported in approved secure containers such as official transport bags or boxes. They must never be transported in dustbin sacks, carrier bags, or unapproved containers. These containers must not be left unattended unless stored in a secure area awaiting collection, and they must only be handled and transported by an approved carrier.

13. Faxing

13.1. As of April 2020, NHS has formally phased out the use of fax machines and as such, person-identifiable information must not be sent via fax unless there is absolutely no alternative in an emergency situation. Faxing is an insecure method of transmission and should only be used as a last resort.

13.1.1. Whenever possible, staff must use secure alternatives such as:

- NHS Mail (which is encrypted and secure for transmitting confidential information).
- Scanning the document and sending it as a PDF attachment via NHS Mail, which also provides an audit trail of the transmission.
- Using an approved secure file-sharing platform in line with NHS CIOS ICB's policies.

13.2. If faxing is the only option in an emergency, additional precautions must be taken:

- Confirm the recipient's fax number in advance and ensure they are ready to receive the document.
- Use a fax cover sheet marked 'Confidential' with the recipient's details clearly stated.
- Call the recipient before and after sending the fax to ensure it has been received securely.
- Only fax the minimum necessary information to meet the request.

13.3. Staff must always seek guidance from the Information Governance (IG) team or the Data Protection Officer (DPO) if they are unsure about secure methods of sending confidential information.

14. Storage of confidential information

14.1. Paper-based confidential information must always be kept locked away and preferably in a room that is locked when unattended, particularly at night and weekends or when the building/office will be un-occupied for a long period of time.

14.2. Computer based information must not be saved onto local hard drives or onto removable media, as this does not provide appropriate protection to confidential information, rather it should be saved onto NHS CIOS ICB secure network.

14.3. Encrypted memory sticks can be provided in some exceptional circumstances with the authorisation of line managers.

15. Disposal of confidential information

15.1. When disposing of paper-based confidential information, including person-identifiable data, it must be kept secure until it can be placed in a confidential waste container or shredded. Confidential information must never be placed in a normal waste bin or general waste sack.

15.2. If you notice an overflowing confidential waste container, report it immediately to the Corporate Governance Team. NHS CIOS ICB has contracted providers for the secure removal and disposal of confidential waste, in accordance with the Waste Regulations 2011.

15.3. Computer hard disks and CDs containing confidential information must be securely destroyed or disposed of by the IT Team within NHS CIOS ICB. This ensures that all data is permanently erased, as reformatted disks can still contain recoverable information. The Cornwall IT Services (CITS) team also provides secure disposal services.

15.4. Patient Identifiable Information must be retained for a specific period before disposal, as outlined in the Records Management Code of Practice for Health and Social Care (NHS England, 2023). This Code sets out:

- The minimum retention periods for both medical and business NHS records.
- The legal requirements for proper records management, archiving, and destruction.

15.5. For further guidance, staff should contact the Corporate Governance Team and refer to NHS CIOS ICB's Records Management Policy.

16. Confidentiality of passwords, PIN numbers, smartcards

16.1. Personal passwords, PIN numbers, and smartcard credentials issued to, or created by, employees must be treated as strictly confidential. These authentication details must not be shared with anyone under any circumstances.

16.2. Passwords and PIN numbers must never be written down or stored in an insecure manner.

16.3. Passwords and PINs must not be easily guessable (e.g., they should not relate to the employee's name, date of birth, or the system being accessed).

16.4. Employees must not attempt to bypass, disable, or override security systems, nor should they attempt to:

- Obtain or use another employee's login credentials.
- Access accounts or systems without proper authorisation.

16.5. Any suspected or attempted security breaches must be immediately reported to the IT Security Manager. Unauthorised access or misuse of login credentials may result in disciplinary action and/or legal proceedings under the Computer Misuse Act 1990 and the Data Protection Act 2018.

17. Emailing confidential information

17.1. The most common cause of unauthorised disclosure of confidential, personal, or sensitive information within the NHS is emails sent to the wrong recipient. To prevent this, staff must take the following precautions when emailing confidential information.

17.2. Before sending an email containing confidential, personal identifiable, or sensitive information, always double-check the recipient's email address to ensure it is correct.

17.3. If you are not 100% certain of the correct email address, you must:

- Use the NHSmail Address Book to select the recipient's address.
- If the recipient is not listed, find an alternative method to confirm the correct address.

17.4. All emails containing confidential information must be clearly marked as "Confidential" in the subject line. If possible, confidential information should not be included in the body of the email but instead:

- Attached as a separate document.
- Password protected if necessary (contact CITS ServiceDesk – Ext 1717 for assistance with file protection).

17.5. Wherever possible, patient identifiers should be removed before sending emails.

17.6. If patient data must be included, send only the minimum necessary information, such as an NHS number without a name or address. However, ensure that the correct NHS number is used to avoid misidentification.

17.7. Confidential information must only be sent to recipients with a legitimate need to know. Always double-check recipient details before sending.

17.8. If sending confidential, personal, or sensitive information outside of NHSmail, you must:

- Type [secure] in the email subject header.

This ensures encryption and security measures are applied before the email leaves NHSmail.

17.9. Further guidance on encryption can be found in the Email Policy.

17.10. Emails must not be used as a filing system. Important emails should be:

- Saved to the appropriate NHS CIOS ICB shared folder.
- If the email contains personal data relating to a patient or employee, it may be considered part of their health record or personnel file (p-file).
- Emails are subject to retention periods and may be disclosed under a Subject Access Request (SAR).

18. Instant messaging services

18.1. NHS CIOS ICB permits the use of approved instant messaging services, such as Microsoft Teams (previously Skype for Business), for internal communication.

18.2. Confidential information must never be shared via unapproved social media or instant messaging services, such as WhatsApp, Telegram, or Signal, due to security and data protection risks.

18.3. While Microsoft Teams and Lync are encouraged for communication within the organisation, these platforms do not record conversations. As such, they do not meet formal record-keeping requirements. Staff must ensure that:

- Decisions, key discussions, or actions are documented in line with the Records Management Policy.
- Sensitive information is recorded in approved NHS systems, not solely in instant messaging conversations.

18.4. For further guidance on appropriate communication tools, staff should refer to the ICB's Information Governance Team.

19. Social Media

19.1. Staff must be aware of their confidentiality obligations when using social media platforms, including but not limited to Facebook, Twitter, LinkedIn, and Instagram.

19.2. The unauthorised sharing of confidential or sensitive information relating to patients, staff, or the organisation on social media may constitute a breach of confidentiality and could result in disciplinary action. This includes:

- Posting patient, employee, or corporate information without authorisation.

- Sharing photos, videos, or details that could identify individuals.
- Commenting publicly on confidential NHS business without approval.

19.3. NHS CIOS ICB uses social media for professional and promotional purposes. Staff seeking to use social media for official NHS business should seek advice from the Communications Team to ensure compliance with NHS policies.

19.4. For further guidance, refer to the ICB's social media policy or contact the Communications Team.

20. Working at home

20.1. NHS CIOS ICB has adapted its working practices to reflect the need for the majority of staff to work from home as far as is required. However, where at all possible, it does not advocate taking person-identifiable information (PII) or records home without appropriate justification. If you believe there is a justifiable reason to do so, you must first seek authorisation from:

- The Data Protection Officer (DPO)
- The Caldicott Guardian
- Your line manager

20.2. If exceptional circumstances require you to take patient or corporate records home, you must:

- Ensure they are securely stored to prevent unauthorised access by family members, housemates, or visitors.
- Take full responsibility for the records while in your possession.
- Log and track the records to ensure they are safely returned to the appropriate NHS system.

20.3. For more information, refer to the Agile Working Policy.

21. Copying of software

21.1. All computer software used within NHS CIOS ICB is regulated by licence agreements. A breach of these agreements could result in legal action against both the organisation and the individual staff member responsible.

21.2. Staff must not:

- Copy, download, or install software from NHS systems for personal use.
- Use unlicensed or unauthorised software on NHS devices.

- Share NHS-licensed software with external parties or install it on personal devices.

21.3. Unauthorised software use is a breach of licensing agreements and may violate the NHS CIOS ICB IT Security Policy. Staff found in violation may be subject to disciplinary action and potential legal consequences.

21.4. For guidance on software use, contact the IT Security Team.

22. Compliance and Monitoring

22.1. **Interpretation -** If any person requires an explanation concerning the interpretation or the relevance of this Code of Conduct, they must discuss the matter with their line manager, Caldicott Guardian, SIRO, DPO, Head of IG or a member of the Human Resources team.

22.2. **Non-compliance -** Non-compliance with this code of conduct by any person working for CIOS ICB may result in disciplinary action being taken in accordance with the ICB disciplinary procedure and may lead to summary dismissal for gross misconduct and/or legal proceedings.

22.3. A record is kept of everyone who accesses information held electronically. This information is capable of being audited and can be made available on request in accordance with HR policies and procedures.

22.4. To obtain a copy of the disciplinary procedure please refer to IRIS, the Document Library or discuss with your manager or the Human Resources team.

23. Monitoring

23.1. Monitoring of compliance with the Code is undertaken and includes random checks or more formal audits undertaken by the ICB's Internal Auditors.

23.2. Confidentiality audits will also be performed by visits to CIOS ICB site and may be carried out by IT staff, security staff, the Corporate Governance or Human Resources teams to ensure the physical security of information.

For linked/referenced documents see below:

http://systems.hscic.gov.uk/infogov/confidentiality

http://systems.hscic.gov.uk/infogov/codes/cop/code.pdf

24. Update and review

24.1. This policy will be reviewed every two years, in line with policy development or sooner should the need arise.

25. Appendix 1: Regulatory Framework

Information Governance currently encompasses the following local, national and legal regulations. The list is not exhaustive.

- Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Confidentiality: NHS Code of Practice
- BS ISO/IEC 27000 series of Information Security Standards
- Caldicott Guardian Manual and Reviews 2006 and 2013
- Common Law Duty of Confidentiality
- Records Management: NHS Code of Practice
- Health and Social Care (Safety and Quality) Act 2015
- Access to Medical Records Act 1988
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Health and Social Care Act 2012 & Health and Social Care (Safety and Quality) Act 2015
- Information Security Management: NHS Code of Practice
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Public Interest Disclosure Act 1998
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Abortion Regulations 1991
- Mental Capacity Act 2005
- NHS Care Records Guarantee
- NHS Constitution
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974

- Re-Use of Public Sector Information Regulations 2005
- Data Security and Protection Toolkit

26. Appendix 2: NHS CIOS Related Policy Documents

This Strategy should be read in conjunction with the following policies and documents:

- Information Governance Strategy
- Information Governance Policy
- Data Protection Policy
- Records Management Code of Practice
- Cornwall Partnership Foundation Trust - Subject Access Request Policy
- Pseudonymisation Policy
- IT Security Policy and all linked policies
- Integrated Identity Management Policy
- Email Policy
- Disciplinary Policy and procedures
- Acceptable Use Policy
- Safe Haven Policy
- Data Quality Policy
- Business Continuity Plans
- Risk Management Strategy and Policy
- Incident Management Policy
- Freedom of Information Policy
- NHS CIOS ICB Privacy Notice
- Home Working Policy
- Information Sharing Protocols and Agreements
- Serious Incident Policy
- Confidentiality Code of Conduct for Employees
- NHS CIOS ICB Information Governance Handbook

This list is not exhaustive.

27. Appendix 3: Equality Impact Assessment

Name of policy to be assessed	Policies relating to Data Protection and Information Governance. Including Confidentiality Code of Conduct, Pseudonymisation Policy, Data Protection Policy, Data Quality Policy, Safe Haven Policy Information Governance Policy, Information Governance Strategy, Records Management Policy.		
Section	Information Governance	**Date of Assessment**	12/02/2019
Officer responsible for the assessment	Data Protection Officer	**Is this a new or existing policy?**	Existing
1. Describe the aims, objectives and purpose of the policy.			
The policies identified above outline how NHS Kernow will meet its legal obligations and NHS requirements and will provide documented evidence of continued commitment to the securing of both corporate and person identifiable information and processes that comply with confidentiality, General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018). The policies provide guidance to staff to ensure the consideration of legal responsibilities and the privacy of all individuals when processing data. The requirements within the Policies are primarily based upon the DPA 2018 which is the key piece of legislation covering security and confidentiality of personal information.			

2. Are there any associated objectives of the policy? Please explain.
Associated objectives are NHS Kernow compliance with the Data Security Protection Toolkit, the attainment of the commitments in the NHS Constitution, Data Protection Act, General Data Protection Regulations, Human Rights Act, Care Records Guarantee and information security standards.
3. Who is intended to benefit from this policy, and in what way?
NHS Kernow staff will benefit from the implementation of robust information security controls to protect them and the information processed as part of the services provided. Patients will benefit from the provision and availability of high quality information and data which meets the Data Protection Act, Freedom of Information Act, Human Rights Act and Records Management: NHS Code of Practice.
4. What outcomes are wanted from this policy?
That the information processed by NHS Kernow and its staff, in all formats, is of a high quality and is protected to the highest possible standards and available quickly, processed in line with legislation and all confidentiality requirements, Government standards and NHS Digital requirements.
5. What factors/ forces could contribute/ detract from the outcomes?

Staff awareness of the content of the policies and staff completing Information Governance training will contribute to information governance practices
6. Who are the main stakeholders in relation to the policy?
The main stakeholders are NHS Kernow Governing Body and its constitutional committees in order to meet its responsibilities. In addition, the Data Protection Officer, the Head of Information Governance, all staff as well as the Information Governance Sub Committee have key operating functions and responsibilities for implementing information governance throughout NHS Kernow. These policies are also important for Individuals in the community.
7. Who implements the policy, and who is responsible for the policy?
The Data protection Officer, Head of Information Governance and the Information Governance Sub Committee providing assurance and escalation to the Workforce Committee.
8. What is the impact on people from Black and Minority Ethnic Groups (BME) (positive or negative)?

Consider relevance to eliminating unlawful discrimination, promoting equality of opportunity and promoting good race relations between people of different racial groups. Issues to consider include people's race, colour and nationality, Gypsy, Roma, Traveller communities, employment issues relating to refugees, asylum seekers, ethnic minorities, language barriers, providing translation and interpreting services, cultural issues and customs, access to services.
The policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of racial groups. The standards of Information Governance, documents referenced in the policies and training will take account of the need to provide data in required formats or languages to ensure accessibility to all to ensure correct use and handling. The new data protection framework protects personal data 'revealing racial or ethnic origin' as a 'special category of data' and processing of it as 'sensitive processing'.
How will any negative impact be mitigated?
A requirement of the information governance programme specifically relates to the provision of information in differing formats and evidence is collated to support this.
9. What is the differential impact for male or female people (positive or negative)?
Consider what issues there are for men and women e.g. responsibilities for dependants, issues for carers, access to training and employment issues, attitudes towards accessing healthcare.

The policies reflect the current national guidance and best practice and is designed to protect the rights of all, irrespective of sex.
How will any negative impact be mitigated?
There are no sections within the policies that distinguish between sexes.
10. What is the differential impact on disabled people (positive or negative)?
Consider what issues there are around each of the disabilities e.g. access to building and services, how we provide services and the way we do this, producing information in alternative formats and employment issues. Consider the requirements of the NHS Accessible Information Standard. Consider attitudinal, physical and social barriers. This can include physical disability, learning disability, people with long term conditions, communication needs arising from a disability.
The policies outline the importance of confidentiality and there should therefore be a positive impact on individuals with a disability as this information should not be shared without the express permission of the individual. The new data protection framework protects personal data 'concerning health' as a 'special category of data' and processing of it as 'sensitive processing'. Additional safeguards are provided throughout the new data protection policies. This may have

an impact on those not capable of, or with varying capacity to, give consent, which is 'freely given, specific, informed and unambiguous', such as people with a learning disability.
How will any negative impact be mitigated?
Adjustments will be made for any member of staff with a disability requiring assistance to enable them to understand how to implement Data Protection to the necessary standards. The standards of Information Governance, documents referenced in the policies and training will take account of the need to provide data in any required format or language to ensure accessibility to all to ensure correct use and handling of corporate and personal information.
11. What is the differential impact on sexual orientation?
Consider what issues there are for the employment process and training and differential health outcomes amongst lesbian and gay people. Also consider provision of services for e.g. older and younger people from lesbian, gay, bi-sexual. Consider heterosexual people as well as lesbian, gay and bisexual people.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the sexual orientation of the individual should be protected. The new data protection framework protects personal data 'concerning sex life and sexual orientation' as a 'special category of data' and processing of it as 'sensitive processing'. The existing condition for processing personal data 'for the purpose of identifying or keeping under review the existence or absence of equality of opportunity' is newly expanded to include personal data concerning an individual's sexual orientation.

How will any negative impact be mitigated?
There are no sections within the policies that will negatively impact an individual due to their sexual orientation.
12. What is the differential impact on people of different ages (positive or negative)?
Consider what issues there are for the employment process and training. Some of our services impact on our community in relation to age e.g. how do we engage with older and younger people about access to our services? Consider safeguarding, consent and child welfare.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the age of the individual should be protected.
How will any negative impact be mitigated?
The policies, their content and implementation will not negatively impact those of differing ages.
13. What differential impact will there be due religion or belief (positive or negative)?

Consider what issues there are for the employment process and training. Also consider the likely impact around the way services are provided e.g. dietary issues, religious holidays, days associated with religious observance, cultural issues and customs, places to worship.
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the impact on those with a religious affiliation or belief should be positive. The new data protection framework protects personal data regarding 'religious or philosophical beliefs' as a 'special category of data' and processing of it as 'sensitive processing'.
How will any negative impact be mitigated?
The policies, their content and implementation will not negatively impact those with a religious affiliation or belief.
14. What is the impact on marriage of civil partnership (positive or negative)? NB: this is particularly relevant for employment policies
This characteristic is relevant in law only to employment, however, NHS Kernow will strive to consider this characteristic in all aspects of its work. Consider what issues there may be for someone who is married or in a civil partnership. Are

they likely to be different to those faced by a single person? What, if any are the likely implications for employment and does it differ according to marital status?
The policies support the protection of personal data, and whilst there may be a requirement to collect personal sensitive data, this should not then be shared inappropriately therefore the impact on marriage or civil partnership status of the individual should be positive.
How will any negative be mitigated?
The policies do not negatively impact those who are married or in a civil partnerships.
15. What is the differential impact who have gone through or are going through gender reassignment, or who identify as transgender?
Consider what issues there are for people who have been through or a going through transition from one sex to another. How is this going to affect their access to services and their treatment when receiving NHS care? What are the likely implications for employment of a transgender person? This can include issues such as privacy of data and harassment.
The policies outline the legal basis for collecting sensitive information, limits how and when it may be shared and when it should be destroyed. They also outline the expectations of staff to maintain confidentiality.

How will any negative impact be mitigated?
No negative impact has been identified for those who gone through or are going through gender reassignment, or who identify as transgender.
16. What is the differential impact on people who are pregnant or breast feeding mothers, or those on maternity leave?
This characteristic applies to pregnant and breast feeding mothers with babies of up to six months, in employment and when accessing services. When developing a policy or services consider how a nursing mother will be able to nurse her baby in a particular facility and what staff may need to do to enable the baby to be nursed. Consider working arrangements, part-time working, infant caring responsibilities.
The Data Protection Policy includes the requirement for training of all staff to Information Governance standards. Information Governance training and all documentation will remain available to staff on maternity leave or on return from maternity leave. Knowledge and skills following maternity leave will be updated using the mandatory training requirements. Staff are required to maintain the code of confidentiality and therefore under these policies are expected not to share information relating to pregnancy or maternity leave without the consent of the individual. The new data protection framework protects personal data 'concerning health' as a 'special category of data' and processing of it as 'sensitive processing'. Additional safeguards are provided throughout the new data protection framework.
How will any negative impact be mitigated?

There is nothing in the policies which would negatively impact those who are pregnant or on maternity leave.
17. Other identified groups:
Consider carers, veterans, different socio-economic groups, people living in poverty, area inequality, income, resident status (migrants), people who are homeless, long-term unemployed, people who are geographically isolated, people who misuse drugs, those who are in stigmatised occupations, people with limited family or social networks, and other groups experiencing disadvantage and barriers to access.
No negative impact has been identified for these groups. However there may be a positive impact in that the policies set out how personal information should be handled and how long it should be retained. The policies also set out the requirements for staff to maintain a code of confidentiality. We also acknowledge and will work with individuals who, in order to exercise their rights, may need to speak rather than write to the CCG formally.
How will any negative impact be mitigated?
No negative impact has been identified.
18. How have the Core Human Rights Values been considered in the formulation of this policy/strategy? If they haven't please reconsider the document and amend to incorporate these values.

- **Fairness;**
- **Respect;**
- **Equality;**
- **Dignity;**
- **Autonomy**

The requirements and principles of the Data Protection Act, which is linked to the Human Rights Act, have been taken into account when writing these policies, including the individual rights of data subjects. Fairness in informing individuals of the uses to be made of their data in a fair processing notice have been produced, respect for privacy, dignity and choice have been written into all Information Governance Policies.

19. Which of the Human Rights Articles does this document impact?

The right:	**Yes / No:**
• To life	No
• Not to be tortured or treated in an inhuman or degrading way	No
• To liberty and security	No
• To a fair trial	No

• To respect for home and family life, and correspondence	Yes
• To freedom of thought, conscience and religion	No
• To freedom of expression	No
• To freedom of assembly and association	No
• To marry and found a family	No
• Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention	Yes
• To peaceful enjoyment of possessions	No
a) What existing evidence (either presumed or otherwise) do you have for this?	
All documentation produced as part of the Information Governance programme of work has taken account of the Human Rights Act and this has been referenced where necessary.	

20. How will you ensure that those responsible for implementing the Policy are aware of the Human Rights implications and equipped to deal with them?
The Act has been referenced within the policies and procedures produced and any monitoring of compliance will include the awareness of patients and staff having a right to privacy, dignity, respect and choice.
21. Describe how the policy contributes towards eliminating discrimination, harassment and victimisation.
By setting out how personal information will be handled and stored and the expectations of staff in these matters information should not be held for the purposes of discrimination, harassment and victimisation. The policies also allow for individuals to rectify information where it is believed to be held incorrectly.
22. Describe how the policy contributes towards advancing equality of opportunity.
The policies describe how and when information should be collected, stored and for how long. This should mean that the organisation does not hold inappropriate information about people without a considered business reason. The code of confidentially sets out how staff should treat information in their care.
23. Describe how the policy contributes towards promoting good relations between people with protected characteristics.

The policies set out how information both personal and corporate will be managed by the organisation. If the policies are followed then those individuals with protected characteristics should be positively impacted as sensitive data can only be collected within a lawful basis and then must be kept confidential.
24. If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services or the working environment for that group of people.
The policies can be provided in multiple formats if necessary.
25. Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
Not applicable
26. If the negative impacts identified have been unable to be mitigated through amendment to the policy or mitigating actions, explain what your next steps are.
Not applicable.

28.