Confidentiality and Data Protection Handbook

Table of contents

1 Introduction

1.1 Handbook statement

As detailed within NHS England's Confidentiality Policy, all staff working in the NHS are bound by a legal duty of confidence to protect personal information they may encounter during their work. This is not purely a requirement of their contractual responsibilities; it is also a requirement within the common law duty of confidence.

This handbook explains and enforces the obligations of confidentiality and non-disclosure among the employees of this organisation. This applies to information generated, held and processed by the organisation. This handbook should be read in conjunction with the organisation's privacy notices and an individual's contract of employment where this contains a confidentiality agreement.

Throughout this document, there are many references to policies and tools that can support this subject. The Confidentiality and Data Protection Handbook will also be supported by the Data Security and Protection Toolkit Handbook and subsequent polices that support the annual DSPT return.

Within the annexes at the end of this handbook are documents for both staff and third parties which are to be used to confirm agreement of compliance. All staff and third parties are to sign to confirm they fully understand the requirement to adhere to confidentiality principles which are designed to safeguard and govern the use of patient information within any health and social care organisation.

1.2 Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage compared to others, in accordance with the Equality Act 2010. Consideration has been given to the impact this handbook might have with regard to the individual protected characteristics of those to whom it applies.

This handbook and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

2 Legislation and guidance

2.1 Supporting information

Throughout this handbook, reference is made to the current NDG Caldicott Guardian guidance and other supporting references. To further support, a complete list of legislation, guidance documents and policies can be found at Annex A.

2.2 Definition of commonly used terms

A definition of terms, detailing key phrases associated with information governance, can be found at Annex B. This annex also details the management roles to support confidentiality and data protection within primary care.

3 Confidentiality requirements

3.1 Principles

This handbook outlines the principles that are to be adhered to by all staff at this organisation so that they understand the requirement for effective control of personal confidential data (formerly known as patient identifiable information).

Staff are to be reminded that information classed as objective knowledge relates to the affairs of the organisation. This may include information regarding the following:

- Partners and directors
- Patients
- Employees
- Contractors
- Decisions
- Contractual arrangements
- Market information
- Dealings
- Transactions
- Technology
- Business associates
- Suppliers
- Policies
- Procedures
- Systems

All employees must, from the beginning of their employment with the organisation, including after the termination of that employment, observe strict confidentiality and non-disclosure in respect of any information held by the organisation, except when required or authorised to disclose such information by the organisation or by law.

The reputation and continuing ability of the organisation to work effectively in the position of trust and responsibility it holds (which is also reflected in the trust and responsibility held by those persons engaged by the organisation to work on its behalf) rely on confidential information being held as confidential. Such information must not be improperly disclosed and must be used only for the purpose for which it was gathered.

There must be no attempt to use any confidential information in a manner that may, either directly or indirectly, cause, or be calculated to cause, injury or loss to the organisation.

Any breach of confidentiality, particularly involving data, could have major negative consequences for this organisation and the individual. The organisation will therefore take the appropriate disciplinary action against any employee who commits a breach of confidentiality by reporting it to the organisation's DPO.

If it is a serious breach, the DPO will be bound to recommend that it is reported to the ICO which may, in turn, institute criminal proceedings against the individual and, if found to be negligent, the organisation itself. The individual, if found guilty, will be required to pay a fine and will acquire a criminal record. The organisation may be heavily fined if found guilty.

Further reading on data breaches and their reporting can be found in Chapter 13.

The Caldicott Principles are derived from the Dame Fiona Caldicott Information Governance Review in 2013, which now forms the current National Data Guardian document titled Guidance about the appointment of Caldicott Guardians, their role and responsibilities.

3.2 Importance of confidentiality

Confidentiality is a fundamental part of healthcare and crucial to the trust between clinicians and patients. Patients entrust this organisation with sensitive personal information relating to their health and other matters in order to receive the treatment and services they require. They should be able to expect that this information will remain confidential unless there is a compelling reason why it should not.

All employees must, from the date of the commencement of their employment or other form of engagement, and thereafter, observe strict confidentiality in respect of any information held by the organisation and by each individual working on behalf of the organisation. This includes dealings, transactions, procedures, policies, decisions, systems and other matters of a confidential nature concerning the organisation and its affairs. Additionally, employees must not, through negligence, wilful misconduct or inadvertence, allow the use, exploitation or disclosure of any confidential information relating to the affairs of the organisation, its patients, partners, employees, contractors, business partners or suppliers.

Some patients may lack the capacity to give or withhold their consent to disclosure of confidential information, but this does not diminish the duty of confidence. The duty of confidentiality applies to all patients, regardless of race, gender, social class, age, religion, sexual orientation, appearance, disability or medical condition.

Information that can identify individual patients must not be used or disclosed for purposes other than direct healthcare, unless the patient (or appointed representative) has given explicit consent, except where the law requires disclosure or there is an overriding public interest to disclose. All patient-identifiable health information must be treated as confidential information, regardless of the format in which it is held. Information that is effectively anonymised can be used with fewer constraints, but controls must be in place to prevent the information becoming re-identifiable at a later date.

3.3 NHS Confidential Code of Practice

All staff at this organisation are to adhere to the principles of confidentiality outlined in the NHS Confidentiality Code of Practice:

- Personal confidential data must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
- Access to personal confidential data must be on a need-to-know basis
- Disclosure of personal confidential data must be limited to the purpose for which it is required
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information, that decision must be justified and documented
- Any concerns about the disclosure of information must be discussed with line management
- Patients at this organisation are to be informed of the intended use of their information and this organisation will adhere to the detailed requirements shown at Annex A to the Code

This organisation will ensure that the requirements within the above Code of Practice are strictly followed, and that staff will report any breaches of confidence or potential risks to the Caldicott Guardian / IG Lead immediately.

3.4 Good practice

The following actions at this organisation will be undertaken to ensure that confidentiality is maintained:

- Personal confidential data will be anonymised as far as is reasonably practicable, whilst being mindful of not compromising the data
- Access to consulting rooms, administrative areas and record storage areas will be restricted
- All staff should always maintain a clear desk, and locked monitor when not in use. No patient confidential information is to be left unattended in any unsecured area at any time. Further reading can be found in the Clear Desk and Clear Screen Policy
- All IT equipment is to be shut down at the end of the working day except for systems that must remain switched on, such as server equipment
- Smartcards are to be removed from the computer whenever the user leaves their workstation. The Smartcard Policy details the need for, and terms and conditions of use of, the NHS Smartcard. Chapter 9 also details the use of smartcards at this organisation
- Confidential waste will be shredded or disposed of appropriately and as detailed within the Confidential Waste Policy

- Staff will not talk about patients or discuss confidential information in areas where they may be overheard

- Compliance audits will be undertaken. This is detailed in Chapter 12

The Communications Policy provides advice on disclosing information electronically or via telephone to a patient, proxy or third party. The NHS Confidential Code of Practice is detailed at Section 4.2.

3.5 Managing confidentiality and data principles

To meet the vision for managing confidentiality and data protection standards there are three key, interlinked aims to the policy, which will ensure the delivery of an effective policy framework.

1	Legal compliance	This organisation aims to meet and exceed all compliance requirements relating to confidentiality and data protection. The organisation will undertake or commission annual assessments and audits of its compliance with legal requirements through the DSPT and demonstrate compliance to all relevant healthcare standards. This document will also show that the organisation has adopted the accountability for demonstrating compliance with the UK GDPR as required by Article 5(2).
2	Information security	This organisation will promote effective confidentiality and security practices to its staff through an Information Security Management System (ISMS) which includes policies, procedures and training. The organisation has established and maintains incident reporting procedures, and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
3	Openness	Non-confidential information relating to this organisation and its services should be available to the public through a variety of media. The organisation will undertake or commission annual assessments and audits of its policies and arrangements for openness through the DSPT.

3.6 Transporting confidential records

There is a requirement for all confidential records to be appropriately managed when being transferred between PCSE & Rockliffe Court Surgery

3.7 Transferring electronic records

General practice offers an array of services to patients to keep up with the demand for greater efficiency and, of course, for better healthcare. Access to and the transfer of healthcare records are required for the following:

- GP online services
- When a patient moves between practices via the GP2GP transfer system
- When remote access is required to a patient's medical record away from the organisation by other healthcare professionals

Further reading relating to the processes and requirements can be found in the Electronic Transfer of and Access to the Healthcare Record.

3.8 Protected information under the Gender Recognition Act

The Gender Recognition Act 2004 at Section 22 states that it is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.

3.9 Right of privacy

Information sharing is affected by the Human Rights Act 1998 Article 8, especially surrounding everyone's right to have a private and family life, within their home and within their correspondence. It remains the responsibility of this organisation to ensure that they have a basis for processing that meets common law requirements and the requirements of DPA18, and for public bodies, that they are acting within their powers.

Further reading can be found in the British Institute of Human Rights guidance titled The right to respect for private and family life, home and correspondence.

3.10 Confidentiality agreements

The following confidentiality agreements are to be read, understood and complied with:

- **Staff confidentiality agreement**

  An employee confidentiality agreement is a contract that prevents the employee from revealing confidential information about the organisation or its patients. All staff have a legal duty of confidence to keep personal confidential data private and not to divulge information accidentally.

  All persons engaged to work for and on behalf of the organisation will be required to sign the confidentiality and non-disclosure agreement to be found at Annex C.

  A signed copy will be held in the individual's personnel file.

- **Third-party confidentiality agreement**

  This organisation is subject to the common law duty to ensure that confidential information is protected from inappropriate disclosure. Furthermore, under Principle 1 of the Data Protection Act 2018, personal information must be processed (disclosed) lawfully. This organisation will only be able to comply with these conditions where it ensures that third parties with whom it has contracts are subject to, and comply with, service user confidentiality, information security, freedom of information and data protection requirements.

  Visitors to the organisation will be expected to sign a Statement of Confidentiality.

  A template third-party confidentiality agreement is available at Annex D.

- **Third-party access to confidential information**

  In addition to the confidentiality agreement, should a contractor be required to access or process confidential information held by this organisation, the contractor shall keep all such information secure at all times, e.g., in a locked cupboard or, where this information is stored electronically, by using appropriate security precautions.

  Any third party shall only process such data in accordance with instructions received from this organisation.

  Contractors must be aware of the possible impact of the Freedom of Information Act 2000 on the documentation connected with the contract.

  The contractor shall indemnify this organisation and the Secretary of State for Health against all claims and proceedings, including liability, loss, costs and expenses incurred in connection therewith, made or brought by any person in respect of any loss, damage or distress caused to that person as a result of the contractor's loss, damage, destruction or unauthorised disclosure of, or unauthorised access to, or the unauthorised and/or lawful processing of any confidential information (including medical records and notes) held by the contractor, its employees or agents.

  The information will, at all times, be the property of this organisation. The original information must be returned to this organisation by the contractor in its entirety on completion of the task for which the information was provided, or on termination of this agreement.

  No copies of the information may be kept by the contractor without the approval of this organisation. The information shall not be removed from this organisation without the appropriate authorisation, subject to the necessary approval, and must be encrypted to the required standard. The contractor must only use and process information for the purpose for which it has been supplied.

Under the Data Protection Act 2018, a breach of confidentiality may constitute an offence which may lead to prosecution.

3.11 Third-party requests for information

Any employee approached by a third party, including any media source, and asked to make comments or provide information relating to the organisation and its affairs (or the affairs of its patients, partners, employees, contractors or any business associate) must not, under any circumstances, respond without having sought permission and guidance from the Practice Manager.

The Practice Manager will then discuss the request with the Partners and should it be a medica request, consider asking for assistance from the press information/media officer at the ICB.

4 Compliance

4.1 Overview

When staff manage any business information, they must comply with all applicable requirements of the procedures undertaken. Therefore, all staff are required to manage information to the highest standards in order to ensure compliance with the appropriate standards. Furthermore, they are to secure all information and promote appropriate information access.

This organisation fully endorses the principles set out in DPA18 and Article 5 of the UK GDPR which sets out the following seven key principles:

Principle	Reference
Lawfulness, fairness and transparency	Article 5 (1) (a)
Purpose limitation	Article 5 (1) (b)
Data minimisation	Article 5 (1) (c)
Accuracy	Article 5 (1) (d)
Storage limitation	Article 5 (1) (e)
Integrity and confidentiality (security)	Article 5 (1) (f)
Accountability	Article 5 (2)

Any breach of the data protection legislation, with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with organisational policy, will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal.

Employees could also face criminal proceedings.

For further detailed information, see the Confidentiality Code of Practice Policy and UK GDPR Policy. Furthermore, a list of policies that support the compliance of the various areas of confidentiality can be found at Annex A.

Audit and assurance are discussed in Chapter 12.

4.2 Staff obligations

All staff must:

- Always endeavour to maintain patient confidentiality
- Not discuss confidential information with colleagues without patient consent (unless it is part of the provision of care)
- Not discuss confidential information in a location or manner that allows it to be overheard by those not involved with the provision of care
- Handle patient information received from another provider sensitively and confidentially
- Not allow confidential information to be visible in public places
- Store and dispose of confidential information in accordance with the DPA18 and the Record Retention Schedule and/or NHS E Records Management Code of Practice
- Not access confidential information about a patient unless it is necessary as part of their work
- Not remove confidential information from the premises unless it is necessary to do so to provide treatment to a patient, the appropriate technical safeguards are in place and there is agreement from the Caldicott Guardian / IG Lead and/or Senior Information Risk Owner (SIRO)
- Contact the Caldicott Guardian / IG Lead or SIRO if there are barriers to maintaining confidentiality
- Report any loss, inappropriate storage or incorrect disclosure of confidential information to the Caldicott Guardian / IG Lead or SIRO
- Comply with the law and guidance / codes of conduct laid down by their respective regulatory and professional bodies
- Read, understand and comply with organisational policies and procedures
- Undertake IG training

4.3 Non-disclosure of information

It is an obligation upon all employees during employment, or those engaged under other contractual arrangements, to maintain information in confidence and not, directly or indirectly, disclose it, other than for the purposes for which it was gathered. Any confidential information in the possession of an individual, either in electronic format or hard copy, shall be returned to the organisation before or at the point in time when employment ceases, however such cessation occurs.

Following the cessation of employment, or other contractual engagement with the organisation, an individual must not, directly or indirectly, use for gain, discuss or pass on to others confidential information that can be classed as objective knowledge in that it has been gained during the course of their employment.

4.4 Abuse of privilege

The NHS Confidentiality Policy states the following:

- It is forbidden for employees to knowingly browse, search for or look at any personal or confidential information 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 of the Data Protection Act 2018

- When dealing with personal confidential data of any nature, staff must be aware of their personal responsibility and contractual obligations and must undertake to abide by the policies and procedures of NHS England

This information is further detailed in the Caldicott and Confidentiality Policy.

4.5 Confidentiality breach

Any breach of confidentiality must be reported to the Practice Manager. All breaches will be recorded and managed in accordance with the Information Commissioner's Office's (ICO) requirements. Full guidance can be found in Chapter 13.

This subject is discussed in detail within the Information Governance Breach Reporting Policy and UK GDPR Policy.

4.6 Safeguarding and confidentiality

When a decision is taken to disclose information about a patient to a third party due to safeguarding concerns/public interest, the patient or their representative should always be told and asked for consent before the disclosure, unless it would be unsafe or impractical to do so. In circumstances where consent cannot be sought, then there must be clear legal reasons and necessity for sharing the information.

The principle of proportionality is also important insofar as only the minimum necessary information should be disclosed to support the objectives of the disclosure. In all cases, a record of the decision-making process must be retained. In general, safeguarding teams should be able to quote their legal powers to exempt their requests from UK GDPR non-disclosure, and the requesting organisation should be asked formally to quote their legal powers. If they have a legal power, consent is not required.

For the purposes of safeguarding, guidance from the Data Protection Act 2018 is to be sought. Specifically, Article 9 refers to the lawfulness of processing, and Article 8 relates to a child's consent. For information relating to criminal convictions and offences, refer to Article 10 of DPA18.

The following legislation is also relevant to support these subjects when considering data protection:

- The Children Act 1989 establishes implied powers for local authorities to share information to safeguard children. Local authorities have a duty to investigate where a child is the subject of an emergency protection order, is in police protection or where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm.

- Under the Children Act 2004, local authorities must make arrangements to promote cooperation with relevant partners and others, to improve wellbeing.

- The Care Act 2014 sets out a clear legal framework for how local authorities and other parts of the system should protect adults at risk of abuse or neglect. Local authorities have a duty to make enquiries where an adult is experiencing, or is at risk of experiencing, abuse or neglect, and they have a duty to collaborate with partners generally and in specific cases.

For further guidance on this subject, refer to:

- DfE guidance titled Information sharing – Advice for practitioners providing safeguarding services to children, young people, parents and carers

- ICO guidance titled A guide to lawful basis

- The Safeguarding Handbook

4.7 Whistleblowing or protected disclosures

In respect of any malpractice or unlawful conduct, nothing in this document prevents an employee or other individual from making a protected disclosure under the Public Interest Disclosure Act 1998 as any employee is entitled to submit a protected disclosure.

This legislation was enacted to enable employees and other persons such as temporary agency workers to disclose genuine concerns, especially those that involve unlawful conduct or malpractice. The legislation also protects them from any form of victimisation arising from making such a disclosure.

Further guidance can be sought from the NHS E document Freedom to Speak Up, and the Freedom to Speak Up Policy and Procedure.

4.8 Healthcare professionals

It is important that healthcare professionals have an understanding of the legal framework and good practice guidance issued by their own professional bodies for sharing information to assist with the following:

- Multi-agency safeguarding enquiries
- Case discussions
- Serious case reviews (SCRs)
- Multi-agency learning reviews (MALRs)
- Domestic homicide reviews (DHRs)

- Safeguarding adults reviews (SARs)
- Multi-Agency Risk Assessment Conference (MARAC)
- Multi-Agency Public Protection Arrangements (MAPPA)
- Vulnerable Adult Risk Management (VARM) meetings

4.9 Privacy notices

The following privacy notices explain how the organisation gathers, uses, discloses and manages data for various groups:

- Privacy Notice – Practice
- Privacy Notice – Children
- Privacy Notice – Employee

4.10 Data Security and Protection Toolkit (DSPT)

This organisation will undertake the DSPT assessment to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal information, thus reducing the number of individuals who 'opt out' of the sharing of their personal confidential data

To demonstrate compliance, this organisation is required to submit the assessment by 30th June annually and use the current Assertions and Evidence items for the Data Security and Protection Toolkit for the relevant year.

4.11 Information Asset Register

An information asset is a repository for similar or specific types of information and these repositories can be either physical or virtual. They include CRM, cloud storage or backup systems, email services or even manual filing cabinets. Any repository where data is stored or processed is deemed to be an information asset.

Data has both value and risk, so from a commercial point of view and a governance point of view, having an Information Asset Register really is essential. It should state who is specifically responsible for each Information Asset, i.e., the Information Asset Owner. For larger organisations, the various assets could have different owners, which should be recorded in the register.

In terms of information governance, the Information Asset Register (IAR) reflects the risks and potential outcomes that are possible, should that asset become lost or compromised. An IAR is a simple way to help understand and manage the organisation's information assets – i.e., what you have, where they are, how they are secured, and who has access to them.

The register must note whether the asset contains personal confidential data and whether that information includes any 'sensitive' or 'Special Category' personal data.

4.12 Compliance with recordings

Recordings refer to audio, videos, photographs and any other type of visual image of patients made by using any recording device, including mobile phones.

The General Medical Council guidance on making and using visual and audio recording of patients advises that when making or using recordings, patients' privacy and dignity must be respected. All clinical recordings created on the organisation's premises and inside patients' homes are subject to this policy, irrespective of who owns the equipment or the materials on which they are produced.

Due to the potential patient safety risks associated with phone, video and online consultations, should there be any concerns relating to any safeguarding issues then the same processes will be followed as detailed within The Safeguarding Handbook and include adding flags or alerts on the at-risk patient's healthcare record. Any safeguarding concerns are to be discussed with the Safeguarding Lead.

Further reading can be found in the Audio, Visual and Photography Policy; this includes information for patients who wish to overtly, or covertly, record conversations and consultations. Additionally, guidance should be sought from CQC GP mythbuster 100: Online and video consultations and receiving, storing, and handling intimate images.

4.13 Using personal IT equipment

Should an employee use personally owned IT equipment for work purposes, they must be explicitly authorised to do so by the CSU.

It must be confirmed that the IT equipment can secure data to the same extent as the corporate IT equipment. Furthermore, the equipment must not introduce unacceptable risks (such as malware) onto the corporate networks by employees failing to secure their own equipment.

4.14 Business continuity

Cyber resilience is a significant factor when considering business continuity, and planning within the organisation is key to supporting any degradation of service. Further reading can be found in the Business Continuity Plan.

4.15 Additional compliance tools

There are further tools that can be used to support compliance:

- Details of annual confidentiality training, and the requirement for it is at Section 1.1
- A confidentiality quiz is available at Annex E
- A confidentiality poster can be found here

5 Patient confidentiality

5.1 Overview

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent, effectively providing individuals with a degree of control over who sees information they provide in confidence.

This duty can only be overridden if there is a statutory requirement, a court order or a robust public interest justification.

On first contact with the organisation, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, or which they specifically do not give permission to receive information.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

In the event a patient lacks capacity to consent to information being shared, staff should check if a person is authorised by a Lasting Power of Attorney (health and welfare) or has been appointed by the Court of Protection to make that decision. The relevant document must be seen. This person can consent on the patient's behalf but must act in the patient's best interest. If no such person has been appointed, then no one can consent on behalf of that patient.

A professional in the care team must assess if it is in the best interest of the patient to share the information. The patient's wishes and feelings, although not determinative, should be the starting point in this assessment.

Information relating to Lasting Power of Attorney can be found in the Access to Medical Records Policy.

5.2 Patients' right to confidentiality

Patients have a right to expect that information about them will be held in confidence by their GP practice. Confidentiality is central to trust between staff and patients and without assurances, patients may be reluctant to give the information the staff need in order to provide good care.

- All information about patients is confidential, from the most sensitive diagnosis to the fact of having visited the surgery or being registered at the organisation. This includes information about patients' families or others associated with them

- Confidential information may not be health related; it can include anything that is private and not public knowledge

- Workers should discuss confidential information only with those in the organisation who need to know

- Only the minimum amount of necessary information should be disclosed

- The duty of confidentiality owed to a person under 16 is as great as the duty owed to any other person

- Workers must not, under any circumstances, disclose patient information to anyone outside the organisation, except to other health professionals on a need-to-know basis, or where the patient has provided written consent

- Workers must not, under any circumstances, disclose confidential information about the organisation to anyone outside the organisation unless they have the express consent of the Practice Manager and/or Partners

- All patients can expect that their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when a person is at grave risk of serious harm)

- Where disclosure of information is required which is non-routine in nature, the patient will, where possible, be fully informed of the nature of the disclosure prior to it being made

- Where the decision is made to disclose information, the decision to do so must be justified and documented

- Personal confidential data must not be used unless absolutely necessary; anonymised data should be used wherever possible

- Workers must be aware of and conform with the requirements of the Caldicott recommendations and UK GDPR principles

- The electronic transfer of any confidential information, once approved by the Practice Manager and/or a Partner, must be transmitted by NHS.net using agreed encryption methods. Workers must take particular care that confidential information is not transmitted in error by email or over the internet

- Workers must not take data from the organisation's computer systems off the premises unless authorised to do so by the Practice Manager and/or a Partner

- Where this is the case, the information must be kept on the worker's person at all times while travelling, and kept in a secure, lockable location when taken home or to another location

- Workers who suspect a breach of confidentiality must inform the Practice Manager and/or a Partner immediately

- Any breach of confidentiality will be considered as a serious disciplinary offence and may lead to dismissal

- Workers remain bound by a requirement to keep information confidential even if they are no longer employed at the organisation. Any breach, or suspected breach, of confidentiality after the worker has left the organisation's employment will be passed to the organisation's lawyers for consideration

  Further reading can be found in the Information Governance Breach Reporting Policy.

5.3 Communicating with patients

The Communication Policy details the necessary process for staff to be able to effectively communicate both internally and externally, and how they are involved in the communication process. Excellent communication is essential to deliver a service that is fit for purpose.

Communicating includes emails, SMS, website, practice leaflet, intranet, internet and social media, telephones, tele/video conferencing, internal messaging and clinical IT system. The policy details the different ways to communicate and the nuances that are required to effectively manage these.

To support those who may have difficulties in communicating, please refer to the following policies:

- Translator and Interpreter Policy
- Reasonable Adjustment Flag Policy
- Accessible Information Standard Policy
- Deaf Patient Access Policy
- Shared Decision-Making Policy

Furthermore, CQC GP mythbuster 20: Making information accessible outlines the actions this organisation is to take to ensure patients' language and communication needs are met.

5.4 Sharing information with patients

Patients have a right to information about the healthcare services available to them, presented in a way that is easy to follow, understand and use. Patients also have a right to information about any condition or disease from which they are suffering. Such information should be presented in a manner that is easy to follow, understand and use, and should include:

- Diagnosis
- Prognosis
- Treatment options
- Outcomes of treatment
- Common and/or serious side-effects of treatment
- Likely timescale of treatments
- Costs where relevant

Patients must always be given basic information about any treatment the organisation proposes to provide, but it is important to respect the wishes of any patient who asks

not to be given detailed information. Providing treatment to a patient who has requested not to be given detailed information puts a considerable onus upon health professionals as, without such information, patients cannot make proper choices as partners in the healthcare process.

Employees should advise patients how information about them may be used to protect public health, to undertake research and audit, to teach or train clinical staff and students, and to plan and organise healthcare services.

Further reading is available in the Access to Medical Records Policy.

5.5 Consent

Consent to treatment means a person must give permission before they receive any type of medical treatment, test or examination. The principle of consent is an important part of medical ethics and international human rights law.

NHS England guidance titled Consent to treatment provides the definitions for the various types of consent. Detailed reading can be found in the Consent Guidance.

5.6 National Data Opt-Out

The National Data Opt-Out allows a patient to choose if they do not want their confidential clinical information to be used for purposes beyond their individual care and treatment to support research and planning.

For full guidance, refer to NHS England's National Data Opt-Out Operational Policy Guidance Document and the National Data Opt-Out Guidance.

5.7 Subject Access Requests (SARs)

There is a recognised procedure by which personal data is disclosed either to the data subject or to their representative.

Any request must be completed within a maximum of one month from the date of receipt and, ordinarily, there can be no fees charged for any such request.

Detailed information is available in the Access to Medical Records Policy.

5.8 Access to deceased patients' medical records

A request for accessing the medical records of a deceased patient is to be managed according to the Access to Health Records Act 1990. Importantly, this is not considered to be a SAR as the information under DPA 18 only refers to living persons.

Detailed guidance can be found in the Access to Deceased Patients' Records Policy.

5.9 Protecting patient information

When staff are responsible for personal information about patients, they must ensure it is effectively protected against improper disclosure at all times. Many improper disclosures are unintentional.

Staff are not to discuss patients where they can be overheard, or leave patients' records, either on paper or on screen, where they can be seen by other patients, unauthorised healthcare staff or the public. Employees are to take all reasonable steps to ensure that any consultation with a patient is private.

5.10 CCTV monitoring

Closed-circuit television (CCTV) monitoring is commonplace to support the safety and security of staff, patients, contractors and visitors. Due to patient confidentiality, where CCTV is used, the system is to have been installed and used in accordance with both the Data Protection Act 2018 and the Surveillance Camera Code of Practice 2013.

The CCTV Monitoring Policy provides detailed information on various aspects of management responsibilities when using CCTV systems.

6 Data mapping and DPIA

6.1 Data mapping

Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable this organisation to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared and where it is stored (including off-site storage if applicable).
Data mapping is linked to the Data Protection Impact Assessment (DPIA) and when the risk analysis element of the DPIA process is undertaken, the information gathered during the mapping process can be used. Data mapping is not a one-person task. All staff at this organisation will be involved in the mapping process, thus enabling the wider gathering of accurate information.

6.2 Data Protection Impact Assessment (DPIA)

A DPIA is the most efficient way for this organisation to meet its data protection obligations and the expectations of its data subjects.

In accordance with Article 35 of the UK GDPR, a DPIA should be undertaken where:

- A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons. The controller shall then, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single

assessment may address a set of similar processing operations that present similar high risks

- Extensive processing activities are undertaken, including large-scale processing of personal and/or special data

DPIAs are to include the following:

- A description of the process, including the purpose
- An evaluation of the need for the processing in relation to the purpose
- An assessment of the associated risks to the data subjects
- Existing measures to mitigate and control the risk(s)
- Evidence of compliance in relation to risk control

It is considered best practice to undertake DPIAs for existing processing procedures to ensure that this organisation meets its data protection obligations. DPIAs are classed as 'live documents' and processes should be reviewed continually.

As a minimum, a DPIA should be reviewed every three years or whenever there is a change in a process that involves personal data.

Further detailed information is available in the UK GDPR Policy.

7 Disclosure

7.1 Disclosing information about patients

When staff manage any business information, they must comply with all applicable requirements of the procedures undertaken. This handbook advises all staff to manage information to the highest standards in order to ensure compliance with the appropriate standards, to secure all organisational information and to promote appropriate information access.

This organisation fully endorses the seven principles set out in the UK GDPR as detailed in Section 4.1. Staff who process personal information must ensure these principles are followed.

7.2 Sharing information with others providing care

Most people understand and accept that information must be shared within healthcare teams in order to provide their care. Therefore, staff are to ensure that patients are aware that personal information about them will be shared within the healthcare team unless they object, and of the reasons for this. It is particularly important to check that patients understand what will be disclosed if it is necessary to share identifiable information with anyone employed by another organisation or agency who is contributing to their care.

Employees must respect the wishes of any patient who objects to particular information being shared with others providing care, except where this would put others at risk of

death or serious harm. Furthermore, anyone to whom personal information is disclosed should understand that it is given to them in confidence, which they must respect.

All staff members receiving personal information in order to provide or support care are bound by a legal duty of confidence, whether or not they have contractual or professional obligations to protect confidentiality.

Circumstances may arise where a patient cannot be informed about the sharing of information – e.g., because of a medical emergency. In these cases, staff must pass relevant information promptly to those providing the patient's care.

7.3 Disclosing information for clinical audit

Clinical audit is essential to the provision of good care. All clinicians who are undertaking clinical practice have a duty to participate in clinical audit. Where an audit is to be undertaken by the team that provided care, or those working to support them, e.g., clinical audit staff, identifiable information may be disclosed, provided that patients have both:

- Been informed that their data may be disclosed for clinical audit, and of their right to object to the disclosure
- Not objected

If a patient does object, then it should be explained why the information is needed and how this may benefit their care. If it is not possible to provide safe care without disclosing information for audit, then this should be explained to the patient along with any other options that are open to them.

Where clinical audit is to be undertaken by another organisation, information should be anonymised wherever that is practicable. In any case, where it is not practicable to anonymise data, or anonymised data will not fulfil the requirements of the audit, express consent must be obtained before identifiable data is disclosed.

Further reading on clinical audit can be sought in Chapter 12.

7.4 Disclosures where express consent must be sought

Express consent is usually needed before the disclosure of identifiable information for purposes such as research, epidemiology, financial audit or administration.

When seeking express consent to disclose, at this organisation staff must ensure that patients are given enough information on which to base their decision – the reasons for the disclosure and the likely consequences of the disclosure. Staff are also to explain how much information will be disclosed and to whom it will be given.

If the patient withholds consent, or consent cannot be obtained, disclosures may be made only where they are required by law or can be justified in the public interest.

Where the purpose is covered by a regulation made under Section 60 of the Health and Social Care Act 2001, disclosures may also be made without patients' consent.

Staff should make a record of the patient's decision, and whether and why they disclosed information.

Should there be any contractual obligation to a third party, such as another company or organisation, then patients' consent to disclose this information must be agreed prior to undertaking any examination or writing a report for that organisation. Clinicians should offer to show patients the report, or give them copies, whether or not this is required by law.

7.5 Disclosure for judicial or other statutory proceedings

The following are reasons to disclose:

a. Disclosures required by law

Staff must disclose information to satisfy a specific statutory requirement, such as notification of a known or suspected communicable disease. Patients are to be informed about such disclosures, wherever that is practicable, but their consent is not required.

b. Disclosures to courts or in connection with litigation

Staff at this organisation must also disclose information if ordered to do so by a judge or presiding officer of a court. However, an objection may be raised to the judge or the presiding officer if attempts are made to compel any disclosure in what appear to be irrelevant matters. This could be matters relating to relatives or partners of the patient who are not parties to the proceedings.
Staff must not disclose personal information to a third party such as a solicitor, police officer or officer of a court without the patient's express consent, except in the circumstances described below.

c. Disclosures to statutory regulatory bodies

Patient records or other patient information may be needed by a statutory regulatory body for investigation into a health professional's fitness to practice. If a concern is being raised about a health professional to a regulatory body, then, wherever practicable, the patient's consent must be obtained prior to disclosing any identifiable information.

Where patients withhold consent or it is not practicable to seek their consent, the GMC (or other appropriate regulatory body) may be contacted, and they will advise on whether the disclosure of identifiable information would be justified in the public interest or for the protection of other patients.

Wherever practicable, this should be discussed with the patient. There may be exceptional cases where even though the patient objects, disclosure is justified.

7.6 Disclosures in the public interest

Personal information may be disclosed in the public interest without the patient's consent, and in exceptional cases where patients have withheld consent, where the

benefits of the disclosure to an individual or to society outweigh the public's and the patient's interest in keeping the information confidential.

In all cases where disclosing information without consent from the patient is considered, staff must weigh the possible harm (both to the patient, and to the overall trust between clinician and patients) against the benefits that are likely to arise from the release of the information.

Before considering whether a disclosure of personal information 'in the public interest' would be justified, staff must be satisfied that identifiable data is necessary for the purpose, or that it is not practicable to anonymise the data. In such cases an attempt to seek patients' consent should still be made unless it is not practicable to do so, for example because of any of the following:

- The patients are not competent to give consent
- The records are of such age and/or quantity that reasonable efforts to trace patients are unlikely to be successful
- The patient has been, or may be, violent; or obtaining consent would undermine the purpose of the disclosure (e.g., disclosures in relation to crime)
- Action must be taken quickly (e.g., in the detection or control of outbreaks of some communicable diseases) and there is insufficient time to contact patients

In cases where there is a serious risk to the patient or others, disclosures may be justified even where patients have been asked to agree to a disclosure but have withheld consent. Staff are to inform patients that a disclosure will be made, wherever it is practicable to do so. Medical records must document any steps that have been taken to seek or obtain consent, and any reasons for disclosing information without consent.

Ultimately, the 'public interest' can be determined only by the courts; but the GMC may also require the requestee to justify their actions should a complaint be made about the disclosure of identifiable information without a patient's consent.

The potential benefits and harms of disclosures made without consent are also considered by the Patient Information Advisory Group when reviewing applications for regulations under the Health and Social Care Act 2001. Disclosures of data covered by Regulation 4 are not in breach of the common law duty of confidentiality.

Disclosure of personal information without consent may be justified in the public interest where failure to do so may expose the patient or others to risk of death or serious harm. Where the patient or others are exposed to a risk so serious that it outweighs the patient's privacy interest, staff are to seek consent to disclosure where practicable. If it is not practicable to seek consent, then information should only be disclosed to an appropriate person or authority.

At this organisation, staff should generally inform the patient before disclosing information. If consent is needed and the patient withholds it, then the reasons for this must be considered.

Should it still be considered that disclosure is necessary to protect a third party from death or serious harm, then any information must be disclosed promptly to an appropriate person or authority. Such situations arise, for example, where a disclosure

may assist in the prevention, detection or prosecution of a serious crime, especially crimes against the person, such as abuse of children.

7.7 Children and other patients who may lack capacity to give consent

The following considerations must be given to the stated circumstances:

a. Disclosures in relation to treatment sought by children or others who lack capacity to give consent

At this organisation, problems may arise if it is considered that a patient lacks capacity to give consent to treatment or disclosure. Any such patients may ask that information about their condition or treatment should not be disclosed to a third party. In these instances, all attempts should be made to persuade them to allow an appropriate person to be involved in the consultation.

Should the patient continue to refuse, but it is believed that, in their medical interests, the disclosure is essential, then relevant information may be disclosed to an appropriate person or authority. In such cases, staff should advise the patient before disclosing any information and, where appropriate, seek and carefully consider the views of an advocate or carer.

All information relating to this conversation must be documented in the patient's record, detailing both discussions with the patient and the reasons for deciding to disclose information.

b. Disclosures where a patient may be a victim of neglect or abuse

Should it be believed that a patient may be a victim of neglect or physical, sexual or emotional abuse and the patient cannot give or withhold consent to disclosure, staff must give information promptly to an appropriate responsible person or statutory agency, where it is believed that the disclosure is in the patient's best interests.

If, for any reason, it is believed that disclosure of information is not in the best interests of an abused or neglected patient, then this is to be discussed with an experienced colleague. If it is then decided not to disclose information, this decision will need to be justified.

c. Disclosure after a patient's death

Staff still have an obligation to keep personal information confidential after a patient dies.

The extent to which confidential information may be disclosed after a patient's death will depend on the circumstances. If the patient had asked for information to remain confidential, the patient's views should be respected.

Where the organisation is unaware of any directions from the patient, the following considerations for information disclosure should be taken into account:

- Whether the disclosure of information may cause distress to, or be of benefit to, the patient's partner or family

- Whether disclosure of information about the patient will, in effect, disclose information about the patient's family or other people
- Whether the information is already public knowledge or can be anonymised
- The purpose of the disclosure

If it is decided to disclose confidential information, then the staff member must be prepared to explain and justify their decision.

Further detailed reading can be sought from the Consent Guidance.

8 Data security and storage

8.1 Overview

It is essential that the organisation has complete and accessible data backups so that in the event of any system failure, data can be restored so that normal operations can be resumed quickly and effectively. It should be noted that these requirements apply to all public sector organisations.

There are also a number of precautions that should be taken to protect the physical security of computers; these will depend on the situation. Different precautions need to be taken for computers used away from the workplace and for laptops used in a variety of locations:

- Personal confidential data is not to be stored on removable devices such as CDs, memory sticks and external hard-drives unless it is encrypted
- Data is not to be downloaded or stored on portable media such as laptops, mobile phones and PDAs unless it is encrypted
- Personal confidential data is not to be stored on PC equipment in non-secure areas unless it is encrypted

Any data stored on a computer hard-drive is vulnerable to the following:

- Loss due to a computer virus
- Physical loss of or damage to the computer, including:
  - Theft
  - Water damage
  - Fire or physical destruction
  - Faulty components
  - Software corruption

In particular, there is a risk of breach of confidentiality where a computer is stolen or otherwise falls into unauthorised hands.

The following precautions should be taken:

- Servers should not be used as regular workstations for any application
- Access to servers will be limited
- Use a shared drive on a networked server for all data wherever possible. All documents are to be saved to the server. The server is backed up daily whereas the C drive on a computer is not backed up and if the computer fails for any reason, the data will be lost
- The clinical server and any other servers that are used to hold clinical information have an automatic backup facility
- No patient data will be stored on a PC or other equipment in non-secure areas
- Use a reputable backup validation service at regular, pre-programmed intervals
- Where a PC is standalone, ensure that the hard-drive is backed up regularly and any confidential data is password protected

Further reading can be found in the Information Governance Breach Reporting Policy.

8.2 Protection against viruses

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from a CD, memory stick or other storage media and by direct links via email and web browsing.

The following precautions will be taken:

- Personal laptops or computers which are not owned by the organisation are not to be connected to the network under any circumstances
- Virus protection software will be installed on ALL computer equipment
- There will be a documented procedure for anti-virus software version control and update, held by NECS
- Automatic or pre-programmed updates will be used wherever possible
- If any viruses are detected, the user of the PC is to stop working on it immediately and inform the Practice Manager, who will advise on future courses of action from this point forward
- Physical restrictions, e.g., drive locks/disable drives, will be used where appropriate
- All staff will be made aware of data security issues in all IT-related protocols and procedures

8.3 Installation of software

Software purchases will be authorised by NECS who will supervise the loading of the software onto the system or individual PCs in accordance with the software licence. Staff are prohibited from installing or upgrading personal or purchased software without the permission of the nominated person. Likewise, they are prohibited from downloading software upgrades or add-ins from the internet without the permission of the nominated person. However, staff are permitted to open files received in the normal course of business, providing they have been received and virus-scanned through the standard virus software installed by the clinical system supplier.

8.4 Hardware

Staff and contractors are not permitted to introduce or otherwise use any hardware or removable storage devices within the organisation, other than that which has been provided or pre-approved by the organisation.

The Practice Manager, via NECS, is responsible for ensuring that the organisation has adequate supplies of removable storage media of a type approved for use. Removable storage media are to be used by authorised staff only.

8.5 Protection against theft or vandalism via access to the building

A security checklist and risk assessment should be undertaken at least annually. An appropriate template is available in Annex F.

In addition, the following precautions should be in place to protect the building:

- Burglar alarm with intruder monitor in each room
- Locks on all downstairs windows
- Appropriate locks, or keypad access only, on all doors
- Separate areas of the building should be sealed off, e.g., the reception area should have shutters and a lockable door, and all separate rooms should be locked when the building is unoccupied
- Where the building is not fully occupied, e.g., during out-of-hours clinics, only the required rooms and corridors should be accessible to the public. Admin areas and consulting rooms not in use are to be kept locked
- Ensure there is a clear responsibility for locking the doors and securing the building when unoccupied
- Ensure any keys stored on-site are not in an obvious place and any instructions about key locations or keypad codes are not easily accessible
- Have a procedure for dealing with unauthorised access during opening hours

- Ensure keypad codes and alarm codes are changed regularly, especially after staff leave employment
- Ensure there is appropriate insurance cover where applicable

- Personal confidential data should never be stored on PC equipment that is not contained in a secure area

- Maintain a separate record of the hardware and software specifications of every PC in the building

- Specific precautions relating to IT hardware are:

    - Use security locks to fix IT hardware to desks to prevent easy removal
    - Locate PCs as far away from windows as possible
    - Clearly 'security mark' all PCs and all parts of PCs, (i.e., tower, monitor, keyboard)
    - Have an asset register for all computer equipment, which includes serial numbers
    - Ensure every PC is password protected

8.6 Accountable suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's Data Security Standards.

The organisation should have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details. An appropriate template list can be found at Annex G.

9 Smartcards

Where access to the clinical or other systems is to be controlled via the issuing of a smartcard, the following will apply:

- Smartcards are issued to an individual on a named basis and are for the use of that person only

- The access level relating to an individual is personal and must not be shared or otherwise made accessible to another member of staff

- The smartcard is to be kept under the personal control of the individual to whom it has been issued at all times and must not be left inserted into a smartcard reader when the individual is not present

- The smartcard will normally be held on a lanyard or other similar device to ensure that it remains with the owner

- On leaving a terminal, the smartcard is to be removed on every occasion

- Staff members are not to leave their smartcards on the premises when they leave work
- Any staff member leaving their smartcard at home will be required to go and collect it
- Staff members sharing smartcards on more than one occasion will be considered for disciplinary action in accordance with the organisation's normal procedures. This would normally be after an informal warning
- Staff members must report the loss of a smartcard to the Practice Manager as soon as it is known that the card is missing
- Smartcards will not normally be handed over between individuals. In the event of a staff member needing to relinquish a card (e.g., over a holiday period), it will be passed back to the Practice Manager or nominated person who will log the transfer and retain the card securely

Further detailed information is available in the Smartcard Policy.

10 Remote access and homeworking

In some instances, it may be appropriate for a member of staff to work at home. Careful consideration needs to be given to the following issues:

- Will the member of staff be using their employer's PC or their own?
- Will the member of staff have dial-in access to the organisation's systems?
- Will the member of staff be using the organisation's confidential data for work purposes, or for the individual's own purposes (e.g., coursework and research)?
- Does the staff member require separate registration under the Data Protection Act?

Under no circumstances will patient or personal confidential data be permitted to be removed from the premises in any format without the express permission of the Data Controller. Work at home is anticipated to relate to administration or non-personal information only.

The following should be considered:

- Physical security of the PC – vulnerability to theft or unauthorised access
- Unauthorised access to confidential data by other family members using the computer
- Risk of loss of the data due to viruses or accidental loss

- Backup of essential data
- Disposal of printouts of confidential data generated at the employee's home
- Ensuring the data is fully deleted from the computer after use
- Ensuring the employee does not use the data for any purpose other than the authorised purpose
- If the work is ongoing, ensuring that the data is destroyed when the employee leaves employment or replaces their home computer
- Ensuring that strong authentication is in place
- Ensuring that data is not held on the computer hard-drive
- Ensuring that up-to-date virus protection is in place

The organisation's responsibilities are as follows:

- The organisation must ensure that the employee fully understands all their responsibilities relating to confidential data. The employee must sign a written statement of the responsibilities they are undertaking regarding the security of the data
- The organisation must be clear as to when it is passing ownership of data to an individual (e.g., for project work or research and development) and this should be authorised by the Caldicott Guardian / Data Controller. The individual may then need to be separately registered under the Data Protection Act 1998
- The organisation is ultimately responsible for ensuring that remote access by staff is managed securely

The Practice Manager's responsibilities are:

- To maintain policy, standards and procedures for remote access, to ensure that risks are identified and appropriate controls implemented to reduce those risks
- To confirm whether remote access to business applications and systems is permitted
- To provide authorisation for all remote access users and the level of access provided
- To ensure that user profiles and log-in access controls are implemented in accordance with agreed access levels
- To assess risks and ensure that controls are being applied effectively

Further detailed information is available in the Home-working Policy and Procedures.

All remote access users are responsible for complying with the contents of this handbook and associated standards, including undertaking the appropriate risk assessments. They must safeguard corporate equipment and information resources and notify the organisation immediately of any security incidents and breaches.

Users must return all relevant equipment on termination of the need to use remote access.

11 Disposal of computer equipment

11.1 Overview

Any redundant computer equipment and data that may be contained in it must be disposed of properly and securely as dictated in The Waste Electrical and Electronic Equipment Regulations 2013.

These regulations are also known as the Hazardous Waste Regulations and Waste Electrical and Electronic Equipment Regulations or WEEE.

11.2 WEEE

The regulations aim to minimise the impact on the environment of the disposal of such items by increasing the proportion that is recycled. They were amended in 2009, mainly concentrating on approved authorised treatment facilities (AATFs).

A number of commercial organisations will dispose of computer equipment on behalf of primary care organisations.

Where an organisation wishes to dispose of computer equipment previously supplied by the ICB, the local coordinator should be approached before arranging for local disposal, as the ICB may have a WEEE-compliant arrangement with equipment suppliers.

11.3 WEEE regulations

Every company that manufactures, imports or brands electrical equipment is known as a “producer” and must have joined an approved producer scheme. A WEEE Producer Registration number is given, which must be passed on to anyone who distributes or sells their equipment.

All new products placed on the market must be marked with this or a similar symbol and their producer number.

11.4 Local disposal

Where equipment is owned by the organisation, the disposal company will be used to collect and dispose of all computer equipment.

Computer equipment, including monitors and base units, is classified as hazardous waste as it contains lead. It is essential that such waste is disposed of only by licensed contractors using approved and licensed waste-receiving sites.

The organisation will only use licensed disposal companies that:

- Track individual items of equipment by serial number from collection through to disposal (whether by recycling or by charitable donation) and retain records following disposal
- Manage an ethical donation scheme of suitable equipment to charities or similar institutions
- Remove any identifying security etchings, markings or labels from the equipment, which have the potential to identify the organisation
- Remove all data and software programs from both fixed and removable media by means of industry-standard software that is SEAP (Security Equipment Assessment Panel) approved, where the equipment is to be reused or donated
- Undertake electrical safety testing of all equipment that is to be donated and certify safety of use, thus indemnifying the organisation
- Destroy all data media (e.g., hard-drives) where the equipment is to be recycled or destroyed
- Provide annual Environment Agency licence documentation and waste control notes on collection of equipment

Further reading can be found in both the Waste Management Policy and Green Plan and Sustainable Development Policy.

12 Audit and assurance

12.1 Overview

With advances in the electronic management of both health and employment information within the NHS, brought about by the advent of the NHS Care Record Service, Electronic Prescribing, Choose and Book, and the Electronic Staff Record, the requirement to monitor access to such confidential information has become increasingly important.

With the large number of staff using these systems, it is imperative that access is strictly monitored and controlled. Furthermore, with the increased use of electronic communications, the movement of confidential information via these methods creates the possibility of information falling into the hands of individuals who do not have a legitimate right of access to it.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented and fulfil their intended purposes may result in a breach of that confidentiality, thereby contravening the requirements of the:

- Caldicott Principles
- Data Protection Act 2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality

The following procedures provide an assurance mechanism by which the effectiveness of controls implemented within the organisation can be audited, areas for improvement and concern highlighted, and recommendations for improved control and management of confidentiality within the organisation can be made.

Further reading can be found in the Quality Improvement and Clinical Audit Policy.

12.2 Monitoring confidential information

In order to provide assurance that access to confidential information is gained only by those individuals who have a legitimate right of access, it is necessary to ensure that appropriate monitoring is undertaken on a regular basis.

Monitoring should be carried out by the organisation in order that irregularities regarding access to confidential information can be identified and reported to the Caldicott Guardian and action taken to address the situation, either through disciplinary action, the implementation of additional controls or other remedial action, as necessary.

Actual or potential breaches of confidentiality should be reported using the organisation's reporting systems.

All areas that manage (process) personal confidential data will be subject to the confidentiality audit procedures. Access to both electronic and manual, paper-based personal confidential data will be audited across the whole organisation, as this will help to capture any inconsistencies.

12.3 Confidentiality audits

These audits can be conducted in a number of ways:

- Interviews with staff using structured questionnaires
- Data Access of Patient Sharing Records on the clinical system
- Notified audit visits with structured questionnaires
- Spot checks at random work areas
- Audit carried out by the Information Asset Owner on electronic or paper-based records
- Staff surveys
- As part of an investigation into a potential breach of confidentiality / data loss

Audits are the responsibility of the management team on a quarterly basis, with any IG breaches reported via the NHS E Data Protection and Security Toolkit, adhering to the Information Governance Breach Reporting Policy.

It is imperative that access is monitored and controlled in an effectual manner. Regular audits must therefore be undertaken to ensure that access to confidential information is gained only by those who are required to access it in the course of their normal duties.

All staff at this organisation have a responsibility to participate in such audits and to comply with the subsequent recommendations.

12.4 Confidentiality audit approach

A spot check audit (see Annex H) should be carried out at least quarterly and will be recorded on the Audit Action Plan Template (see Annex I).

Circumstances when an ad hoc audit may be required include: a potential breach of confidentiality, a change of Information Asset Owner (system owner), data being migrated to another system or a major change to an information asset.

Supporting information to help manage IT assets can be found at:

- Information Asset Owner (IAO) and Information Asset Administrator (IAA) Guidance
- Information Asset Register
- Asset Register (Non-Hardware)
- Hardware Asset Register – Information Governance
- Information Governance Breach Reporting Policy

12.5 Responsibilities

It is the role of the Caldicott Guardian to define the policy in respect of confidentiality audits, taking into account legal requirements.

The Confidentiality Audit Lead is responsible for:

- Providing advice and guidance on confidentiality issues
- Raising awareness of confidentiality, and
- Ensuring that there is ongoing compliance with this handbook and its supporting standards and guidelines

All risks, issues and recommendations identified will be brought to the attention of staff concerned in the first instance, where applicable. In all cases, an agreed action plan will then be implemented and delivery reported through the management team.

Where very significant risks or concerns are identified, immediate remedial action will be taken with the agreement of the audit owner and/or SIRO. Where there is a concern that staff are not complying with appropriate policies, this may be referred as a disciplinary matter. If suppliers are found not to be complying with their contractual terms and conditions of service, this may lead to an early performance review.

The management team are responsible for ensuring that policies are implemented and monitored.

12.6 Non-compliance

Where non-compliance is observed, this should be recorded as soon as possible and should be sufficiently detailed, including all the facts and referring to any relevant evidence. The detail recorded should include an outline of what was observed, where it was observed, who was involved, the date of the observation and why it was considered to be non-compliant.

Each non-compliance observed should have an associated recommendation which should be discussed and agreed with the management team. Non-compliance can fall into one of two categories:

1. Major non-compliance would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequences

2. Minor non-compliance could include one-off occurrences of non-compliance, and occurrences where there is little risk of the non-compliance causing more than a minor irritation

Where a number of minor instances of non-compliance are observed by the same person or the same functional area, this may indicate a more serious problem within that area. If this is the case, these instances of non-compliance should be combined into a major non-compliance.

Failure to comply with the standards and appropriate governance of information, as detailed in this handbook and supporting documents, can result in disciplinary action. All staff are reminded that they are personally responsible for several aspects of legal compliance. Failure to maintain these standards can also result in criminal proceedings against the individual.

12.7 Audit follow-up

Once the audit process is complete, arrangements should be made for follow-up checks where non-compliance has been observed. This will allow the organisation to confirm that the recommended corrective action has been implemented.

13 Breach reporting

13.1 Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data, as detailed within the ICO guidance titled Personal data breaches: a guide.

13.2 Reporting a data breach

Any breach must be reported to the Information Governance Lead. In order to determine the need to inform the ICO of a breach, the Information Governance Lead is to read this supporting guidance and complete the incident reporting form on the DSPT within 72 hours of the breach being identified.

All breaches must be reported without undue delay to the Information Governance Lead / Caldicott Guardian or SIRO, utilising the appropriate breach reporting form, to allow time to meet the DSPT reporting requirements.

Further detailed information is available in the Information Governance Breach Reporting Policy.

13.3 Notifying a data subject of a breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e., a breach that is likely to have an adverse effect on an individual's rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The primary reason for notifying a data subject of a breach is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, the data controller at this organisation is to provide the data subject with the following information in a clear, comprehensible manner:

- The circumstances surrounding the breach
- The details of the person who will be managing the breach
- Any actions taken to contain and manage the breach
- Any other pertinent information to support the data subject

For further detailed guidance, see the Information Governance Breach Reporting Policy.

14 Training requirements

14.1 Information governance training

This organisation is committed to the provision of information governance training and education to ensure the workforce is informed, competent, prepared and possesses the necessary skills and knowledge to perform and respond appropriately to the demands of clinical care and service delivery.

The organisation has a mandatory training programme which includes maintaining awareness of information governance, data protection, confidentiality and security issues for all staff. This is carried out through regular training sessions covering the following subjects:

- Personal responsibilities
- Confidentiality of personal information
- Relevant information governance policies and procedures
- General good practice guidelines covering security and confidentiality
- Records management

The SIRO will direct the Information Governance Lead to take action as necessary to comply with the legal and professional obligations set out in the key national guidance issued by appropriate commissioning bodies.

This includes the requirement for all staff to complete annual information governance training commensurate with their duties and responsibilities. Furthermore, all new starters will be given information governance training as part of the mandatory induction process.

15 Considerations

15.1 Organisational considerations

This organisation will generally assume vicarious liability for the acts of its staff, including those on honorary contracts. However, it is incumbent upon staff to ensure that they:

- Have undergone any suitable training identified as necessary under the terms of this handbook
- Have been fully authorised by their line manager to undertake the activity
- Fully comply with the terms of any relevant organisational policies and/or procedures at all times
- Only depart from any relevant organisational guidelines providing that such departure is always confined to the specific needs of individual circumstances. In healthcare delivery, such departure shall only be undertaken where, in the judgement of the responsible clinician, it is fully appropriate and justifiable. Such a decision is to be fully recorded in the patient's notes
- Staff contracts of employment are produced and monitored by the organisation. All contracts of employment include a data protection and general confidentiality clause as part of controls to enhance privacy and information governance. Agency and contract staff are subject to the same rules
- Confidentiality compliance will be continually monitored, and any findings and subsequent recommendations will be discussed with staff

15.2 Staff considerations

All staff are required to:

- Keep confidential any information regarding patients and staff, only informing those who have a need to know. In particular, telephone conversations and electronic communications must be conducted in a confidential manner. Confidential information must not be disclosed to unauthorised parties without prior authorisation by a senior manager

- Not process any personal information in contravention of DPA18

- Be familiar with and comply with the confidentiality clause in their contract of employment. This organisation has an approved data protection and confidentiality clause in all contracts with third-party contractors and suppliers that process personal information

- Be conversant and comply with all matters concerning confidentiality. Failure to do so could have far-reaching effects on the confidence that patients have in the organisation's staff and their relationships with health professionals

- Understand the importance of being aware of the action to be taken if they receive a request for information from third parties, and the procedure to follow in the event that they wish to make a protected disclosure (whistleblowing)

- Be aware of the Caldicott Principles and that they have a duty to ensure they always remain compliant, as confidentiality is the basis of trust between the patient and this organisation. All staff must ensure they are aware of their individual responsibilities and their duty to always maintain patient confidentiality

It should be noted that:

- To sign the Staff Confidentiality and Non-disclosure Agreement at Annex C, the individual is reminded of the possible outcomes and effects that failure to comply could have on the organisation, and the potential for the individual to acquire a criminal record

- Any breaches of these requirements will potentially be regarded as serious misconduct and, as such, may result in disciplinary action

- Any questions relating to this handbook should be directed to the Practice Manager in the first instance

Annex A – Legislation, guidance and supporting policies

Legislation:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Public Interest Disclosure Act 1998
- National Health Service Act 2006
- The Health and Social Care (National Data Guardian) Act 2018
- Data Protection Act 2018 incorporating UK GDPR at Chapter 2
- EU General Data Protection Regulation as incorporated in English law by the EU (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (the "UK GDPR")

Guidance:

- Caldicott Principles: A consultation about revising, expanding and upholding the principles
- Caldicott review: Information: to share or not to share? The Information Governance Review
- The Caldicott Principles
- The Caldicott Committee Report on the Review of Patient-Identifiable Information
- National Data Opt-out
- NHS Data Security and Protection Toolkit
- Records Management Code of Practice
- The NHS Confidentiality Code of Practice
- NHS IGA GDPR Guidance
- Information Security Management: NHS Code of Practice

Annex B – Definition of terms

Anonymised data

Data which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode, date of birth and any other detail or combination of details that might enable identification.

Anonymised data is not considered ‘personal data’ and is not subject to DPA18.

Caldicott Guardian and/or Information Governance Lead

A Caldicott Guardian, as outlined in the Manual for Caldicott Guardians, is a senior person within a health or social care organisation who ensures that personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. They are responsible for ensuring that personal confidential data is only shared in an appropriate and secure manner.

This organisation is required to have its own Caldicott Guardian, and this is normally a senior clinician. This role is given an additional title of Information Governance (or IG) Lead. Should a non-clinical person be appointed as the Caldicott Guardian, they should be supported by an appropriate clinician.

The Caldicott Guardian's main concern is information relating to individuals and their care. This need for confidentiality also extends to relatives, staff and other individuals. At this organisation, we store, manage and share personal information relating to staff, and the same standards are applied to their information as are applied to the confidentiality of patient information.

Further information can be sought from:

- Manual for Caldicott Guardians as this details the role of the Caldicott Guardian
- The National Data Guardian (NDG) document Guidance about the appointment of Caldicott Guardians, their role and responsibilities
- UK Caldicott Guardian Council

All staff are to be aware of who the Caldicott Guardian / Information Governance Lead is. This information should be added to the Responsible persons list and made freely available.

The nominated lead has responsibility for project managing the overall coordination, publicising and monitoring of the Information Governance Framework, producing performance monitoring reports and ensuring that the annual Data Security and Protection Toolkit (DSPT) return has been submitted on behalf of the organisation.
Information on DSPT can be sought in Section 4.10 and within the Data Security and Protection Handbook.

Caldicott Principles

The eight Caldicott Principles apply to the use of confidential information within health and social care organisations, and to the sharing of such information with other
organisations and between individuals, both for individual care and for other
purposes.

For more information, refer to the Caldicott and Confidentiality Policy.

Consent

NHS England's guidance titled Consent to treatment provides definitions of the various types of consent. Further reading can be found in the Consent Guidance.

Confidential information

Any information processed by the organisation, or supplied (whether in writing, orally or otherwise) by the organisation, or gathered by an individual in relation to the performance of their duties, that is marked as 'confidential'.

Confidential information relating to patients is defined in NHS E's operational guidance document and is also defined in the National Health Service Act 2006.

Data controller

At this organisation, the role of the data controller is to ensure that data is processed in accordance with Article 5 of the UK GDPR. The organisation should be able to demonstrate compliance, and is responsible for making sure data is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Data processor

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that it meets at least one of the bases for lawful processing as stated in Article 6 of the UK GDPR.

Data Protection Act and UK GDPR

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK General Data Protection Regulation. The UK GDPR came into effect on 1st January 2021 and is now incorporated in the DPA 18 at Chapter 2.

Following Brexit, the UK GDPR replaced the EU GDPR. Further reading can be found in the UK GDPR Policy.

Data Protection Officer (DPO)

This supporting role is key to ensuring that the organisation can demonstrate it complies with the UK GDPR. Further details for this role can be found in the Information Commissioner's Office (ICO) guidance titled Data protection officers.

Data Security and Protection Toolkit (DSPT)

The NHS Data Security and Protection Toolkit version 7 (2024/25) is an online self-assessment tool that enables this organisation to assess its performance against the ten data security standards of the National Data Guardian. DSPT is a mandatory requirement which will ensure compliance in line with the UK GDPR.

The Data Security and Protection Toolkit Handbook details the requirements for the annual 30th June deadline when the DSPT is required to be submitted.

Healthcare purposes

Such purposes include all activities that directly contribute to the diagnosis, care and treatment of an individual, and the audit / assurance of the quality of the healthcare provided.

Information Asset Owner and Administrator

Information Asset Owners (IAOs) will be identified for every electronic system and network folder held within this organisation.

The IAO will be responsible for understanding and addressing what information is held within their business area, what is added, what is removed, risks to the security and quality of data held within these systems including compliance with relevant legislation and adherence to national standards in order to provide the relevant assurances to the Caldicott Guardian and SIRO. An IAO will be responsible for an information asset in terms of:

- Identifying risks associated with the information asset
- Managing and operating the asset in compliance with policies and standards
- Ensuring the controls implemented manage all risks appropriately

The Information Asset Administrators (IAAs) work on a daily basis with information contained in an information asset. They have responsibility for the asset to ensure that policies and procedures are applied and adhered to by staff and can recognise actual or potential security incidents relating to their information asset.

They are responsible for reporting such incidents to their IAO and consulting the IAO on incident management. It is possible that the IAO of an information asset is also the IAA of that asset.

Further detailed information is available from the IAO and IAA Guidance.

Information Commissioner's Office (ICO)

For a full overview of the ICO role, please refer to their website here.

Information governance

Information governance, or IG, is the organisational practice of managing information, from its creation to its final disposal, in compliance with all relevant information rights legislation. IG is focused on ensuring that standards and services are introduced to ensure that organisational information is managed securely, is compliant with legislation, and available for access by both staff and external parties, including the public and regulators.

A full list of the policies to support Information Governance can be sought at Annex A.

Medical purposes

As defined in the DPA, these are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and the management of healthcare services.

National Data Opt-Out

The National Data Opt-Out was introduced in England along with both DPA18 and EU
GDPR on 25th May 2018. This followed recommendations from the NDG that patients should be able to opt out of their personal confidential data being used for purposes other than their direct medical care.
Further reading can be sought from the National Data Opt-Out guidance document.

Patient confidential data

Defined in the DPA as information that relates to a living individual who can be identified from that data, or from the data and any other information that is in the possession of, or is likely to come into the possession of, the Data Controller – e.g., name, address, postcode, date of birth, NHS number.

This is as defined in NHS E's Confidentiality Policy.

Primary use of data

Data purposes that directly contribute to the safe care of the patient or service user and include care, diagnosis, referral and treatment processes, together with relevant supporting administrative processes, such as clinical letters and patient administration, and managing appointments for healthcare.

Primary use also includes the clinical audit / assurance of the quality of the healthcare provided, drug safety and public health surveillance.

Protected disclosure

The protected disclosure of unlawful conduct, malpractice or wrongdoings within the organisation is known as whistleblowing, now more commonly known as Freedom to Speak Up.

Further reading about protected disclosure can be found in the Freedom to Speak Up Policy and Procedure.

Pseudonymisation

This provides information to a secondary holder, which is anonymised in that it cannot reasonably be used by this secondary holder to identify an individual. However, it differs from anonymised information in that the original provider of the information may retain a means of identifying individuals.

This will often be achieved by attaching codes or other unique references to the information, so that the data will only be identifiable by those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

Secondary use of data

The use of patient or service user data that does not directly contribute to the safe care of the individual. This includes uses such as performance management, commissioning and contract monitoring, none of which require the identity of the patient or service user.

Senior Information Risk Officer (SIRO)

The SIRO has accountability for ensuring that effective systems and processes are in place to address the IG agenda, including records and document management. This role has overall ownership of information risk and acts as the focal point for information risk management within the organisation.

The SIRO provides advice to the Caldicott / IG Lead on the content of the annual DSPT declaration.

Sensitive personal data

Defined in the DPA as personal data consisting of information relating to:

- Race or ethnic origin
- Political opinions
- Religious beliefs
- Membership of a trade union
- Physical or mental health condition (health record)
- Sexual life
- Commission or alleged commission by the individual of any offence
- Any proceedings for any offence committed or alleged, the disposal of such proceedings, or the sentence of any court in such proceedings

UK Caldicott Guardian Council (UKCGC)

The UK Caldicott Guardian Council is the national body for Caldicott Guardians in the UK. The UKCGC provides support for Caldicott Guardians and others fulfilling the Caldicott function within an organisation.

The UKCGC helps to uphold the eight Caldicott Principles, as detailed in Section 3.1.

Annex C – Staff Confidentiality and Non-Disclosure Agreement

I confirm that I have read and understand the Confidentiality and Non-Disclosure Policy and agree to abide by it.

I understand that any breach of this agreement could result in this organisation's sensitive and confidential data being disclosed to the public or other interested parties and may result in my summary dismissal under the organisation's disciplinary procedure. Furthermore, any such conduct on my part which results in an unauthorised disclosure of confidential personal data may render me liable to being reported to the Information Commissioner's Office (ICO).

The ICO may, in turn, institute criminal proceedings against me and, if I am found guilty by a court of law, I could be fined, and this may also result in a criminal record.

Signed:	
Name (printed):	
Date:	

Annex D – Third-Party Confidentiality Agreement

THIRD-PARTY CONFIDENTIALITY AGREEMENT

(Including Data Protection and Information Security)

During the course of your association with this organisation, you may have access to, see, or hear confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. Unless acting on the instructions of an authorised officer within this organisation, on no account should such information be divulged or discussed with anyone.

Breach of confidence, including the improper passing on of confidential data, could result in this organisation taking action against you.

DEFINITIONS

- **Data Protection Legislation** means (i) the DPA 1998 (ii) the GDPR, the LED and any applicable national laws as amended from time to time (iii) the DPA 2018 (iv) all applicable law concerning privacy, confidentiality or the processing of personal data including, but not limited to, the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

- **Data Protection Officer** shall take the meaning given in the Data Protection Legislation
- **DPA 1998** means the Data Protection Act 1998
- **DPA 2018** means the Data Protection Act 2018
- **GDPR** means the General Data Protection Regulation (Regulation (EU) 2016/679)

  UK GDPR means the UK component that was subsumed into DPA18 (Part 2) following Brexit and incorporated into UK law on 1st January 2021
- **Law** means any law or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bylaw, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the organisation is bound to comply
- **LED** means the Law Enforcement Directive (Directive (EU) 2016/680). Note, this is still relevant post Brexit and is incorporated in the UK GDPR
- **Controller** shall take the meaning given in the Data Protection Legislation
- **Criminal offence data** means personal data relating to criminal convictions and offences or related security measures
- **Personal data** shall take the meaning given in the Data Protection Legislation
- **Processor** shall take the meaning given in the Data Protection Legislation
- **Processing** and cognate terms shall have the meaning given in the Data Protection Legislation
- **Protective measures** means appropriate technical and organisational measures, which may include: pseudonymising and encrypting personal data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to personal data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of such measures
- **Special categories of personal data** shall take the meaning given in the Data Protection Legislation

- **Sub-processor** means any third party appointed to process personal data on behalf of the organisation related to this Agreement

- **Supplier personnel** means any and all persons employed or engaged from time to time in the provision of services and/or the processing of personal data, whether employees, workers, consultants or agents of the organisation or any subcontractor or agent of the organisation

- **Working day** means a day other than a Saturday, Sunday or bank holiday in the UK

Without limiting the generality of the above, for the purpose of this agreement, “confidential information” means and includes any information relating to this organisation, its business and activity including, but not limited to, person and patient identifiable information and other sensitive information in whatever form but excluding any matter that has become public knowledge or part of the public domain. It also includes all other information provided to you which is either labelled or expressed to be confidential, or given to you in circumstances where one would expect the information to be confidential to this organisation.

The third party shall, in relation to any personal data processed in connection with its obligations under this Agreement, process that personal data only in accordance with the instructions set out by this organisation, unless the third party is required to do otherwise by law. If it is so required, the third party shall promptly notify this organisation before processing the personal data unless prohibited by law.

You should also be aware that, regardless of any action taken by this organisation, a breach of confidence could result in a civil action against you for damages.

By signing this Agreement, you undertake:

- To treat as confidential any information that you may come into contact with during the course of your association with this organisation and thereafter

- To only access areas where confidential information is held if permissions are granted

- To respect the rights of patients who may not wish others (i.e., their friends or relatives) to know that they have visited this organisation

Any breaches of this Agreement will be reported to the Caldicott Guardian of this organisation for investigation.

The third party shall, in relation to any personal data processed in connection with its obligations under this Agreement, ensure that it takes all reasonable steps to ensure that third-party personnel are subject to appropriate confidentiality undertakings with the third party or any sub-processor. These should be in writing and legally enforceable.

SECURITY MEASURES

Taking into account the cost of implementation, and the nature, scope, context and purposes of processing, as well as the varying likelihood and severity of risk to the rights and freedoms of natural persons, the third party shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate:

- The pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing

ENGAGING SUB-PROCESSORS

Before allowing any sub-processor to process any personal data related to this Agreement, the third party must:

- Notify this organisation in writing of the intended sub-processor and processing
- Obtain the written consent of this organisation
- Enter into a written agreement with the sub-processor which gives effect to the terms set out in this Agreement, such that they apply to the sub-processor (and in respect of which this organisation is given the benefits of third-party rights to enforce the same)
- Provide this organisation with such information regarding the sub-processor as this organisation may reasonably require

The third party shall remain fully liable for all acts or omissions of any sub-processor.

SUBJECTS' RIGHTS

The third party must assist this organisation by taking appropriate technical and organisational measures, as far as this is possible, for the fulfilment of this organisation's obligation to respond to requests for exercising rights granted to individuals by the Data Protection Legislation.

UK GDPR COMPLIANCE

The third party must assist this organisation in ensuring compliance with the obligations set out in Articles 32 to 36 of the UK GDPR and equivalent provisions implemented into law, taking into account the nature of processing and the information available to the third party.

DELETION OR RETURN OF DATA

The third party shall, in relation to any personal data processed in connection with its obligations under this Agreement, at the written direction of this organisation, delete or return the personal data (and any copies of it) to this organisation on termination of the Agreement, unless the third party is required by law to retain the personal data.

If the third party is asked to delete the personal data, the third party shall provide this organisation with evidence that the personal data has been securely deleted in accordance with the Data Protection Legislation within a period agreed within the written direction of this organisation.

UK GDPR RECORD OF PROCESSING

The third party must create and maintain a record of all categories of data-processing activities conducted under this Agreement, containing:

- The categories of processing carried out under this Agreement
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards

- A general description of the protective measures taken to ensure the security and integrity of the personal data processed under this Agreement

- A log recording the processing of personal data in connection with this Agreement, comprising, as a minimum, details of the personal data concerned, how the personal data was processed, where the personal data was processed and the identity of any individual conducting the processing

The third party shall ensure that the record of processing maintained in accordance with this agreement is provided to this organisation within two working days of a written request.

This contract does not relieve the third party of any obligations conferred upon them by the Data Protection Legislation.

DATA PROTECTION OFFICER

The third party shall designate a Data Protection Officer if required by the Data Protection Legislation and shall communicate to this organisation the name and contact details of any Data Protection Officer.

I have read, understood and agree to comply with this Third-Party Confidentiality Agreement.

Description	Details
Subject matter of the processing	*This should be a high level, short description of what the processing is about, i.e., its subject matter*
Duration of the processing	*Clearly set out the duration of the processing, including dates*
Nature and purpose of the processing	*Please be as specific as possible, but make sure you cover all intended purposes.*

	The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means), etc. *The purpose might include employment processing, statutory obligation, recruitment assessment, etc.*
Type of personal data	*Name, address, date of birth, NI number, telephone number, pay, images, biometric data, etc.* *You should be clear about what data is being used for each purpose you have outlined above.* *You should identify whether you are processing any special categories of personal data or any criminal offence data.* *The special categories of personal data are very similar to sensitive personal data under the DPA 1998.* *They are set out in Article 9. The special categories of personal data are:* • *Race* • *Ethnic origin* • *Political opinion* • *Religion or philosophical belief* • *Trade union membership* • *Genetics* • *Biometrics (where used for ID purposes)*

	• *Health (including mental health)* • *Sex life* • *Sexual orientation* *Unlike under the DPA 1998, personal data relating to criminal convictions and offences are not included. However, similar extra safeguards apply to criminal offence data, which includes data about criminal allegations, proceedings or convictions that would have been sensitive personal data under DPA 1998, and also personal data linked to related security measures.* *You should identify if you are processing this type of data and, if so, seek further advice from your local Information Governance team before the data is processed.*
Categories of Data Subject	*Staff (including volunteers, agents, and temporary workers), customers / clients, suppliers, patients, members of the public, users of a particular website, etc.)*

Name	
Job title	
Employer's name	
Employer's address	
Employer's telephone number	

Name of Line Manager	
Signed	
Approved by	
On behalf of the organisation	
Date	
Third-party signature	

Annex E – Confidentiality quiz

Scenario 1:

A male patient finishes his consultation with the ANP and, as he is leaving, he asks the reception team if it is OK for him to pick up his 16-year-old daughter's prescription.

How do you respond?

Could there be any medication that the daughter may not want her father to see?

You are not permitted to let the patient collect his daughter's prescription without her explicit consent. You have a duty to protect confidential information.

There may be contraception medication that the daughter does not want her father to know about.

Scenario 2:

A 15-year-old girl has attended a GP appointment for a review of her asthma. During the consultation she asks the GP for advice about oral contraception and, when questioned about sexual activity, she advises that she is sexually active but has not told her mum or dad.

Can the GP breach her confidence and, if so, why?

Yes, on child protection/safeguarding grounds. However, if the GP deems the patient has shown maturity and fully understands the consequences of her request and subsequent actions, her confidence should be upheld.

Scenario 3:

You work in a rural organisation, and it is a very close-knit community where everyone helps one another. You see your neighbour in the waiting room and notice that after his appointment he appears upset and leaves without saying anything.

Can you check his clinical record to see if there is anything you can do to help?

No, as you have no legitimate purpose for doing so. If you were to search his record, this would constitute a breach of confidentiality and a breach of the Data Protection Act 2018.

Scenario 4:

You have arranged for a patient to collect a printed copy of their medical notes for an insurance matter. You are off to lunch in five minutes and decide to leave the notes (not in an envelope) on the reception desk.

Is this appropriate?

No, you are failing to protect against improper disclosure and this goes against the NHS Code of Practice 2003. Leaving the notes in such a position means they would be visible to other staff members and patients. You must never leave patient confidential information in an unsecured area at any time.

Scenario 5:

A male patient, aged 14, attends the organisation and asks for a copy of his medical records.

How do you respond?

Patients under the age of 16 are entitled to see or be given a copy of their records if they have the competence to understand the nature of the request. However, they need to be deemed Gillick competent and, as such, need to be assessed by a healthcare professional before being given a copy of their notes.

Scenario 6:

You are handing over to your colleague at reception who is covering your lunch break. You tell them that earlier in the morning you were advised that a patient who had been with the organisation for 55 years had passed away.

You wanted to let them know, as you knew they had known the patient for a long time.

Is it OK to do so?

Staff do need to know of deceased patients, as this prevents unnecessary phone calls being made or letters being sent, thereby causing further upset to the family of the deceased. However, staff must not talk about patients or confidential information in areas where they may be overheard.

Scenario 7:

You answer the phone, and the caller asks for the results of their latest cholesterol test.

What do you need to do?

You should ask the patient to confirm their name, address and date of birth. You can also ask them when they had the test done. Additionally, you could ask further questions to confirm the ID of the caller, such as when they were last in the organisation before their blood test appointment.

This helps you to ascertain whether it is the patient calling or if it is someone else. If there is any doubt, tell the caller you will ring them back.

Scenario 8:

Your organisation is holding a group consultation for diabetic patients, and this is the first group consultation at your organisation. The ANP calls from the meeting room upstairs and asks you to send the six patients who are waiting.

How do you do this?

All six patients would have consented to attend a group consultation, but there will be other patients in the waiting room, and you need to protect the confidentiality of the patients. So, rather than saying, 'Those who are here for the diabetic clinic, please proceed to the meeting room,' you could say, 'All patients here for the group consultation, please proceed to the meeting room.'

You have called no names out and you have not disclosed what the group consultation is about. You have therefore maintained confidentiality as far as is reasonably practicable.

Scenario 9:

You take a call from a patient who wants to confirm their appointment with the visiting mental health nurse, but it is a really bad line.

What do you do?

Option A: Try to confirm the patient's details including name, date of birth, address and who their appointment is with by repeating this information to the patient.

Option B: Advise the patient that they need to call back as you are unable to hear them.

Option B – If you were to repeat everything, all the patients in the waiting area may hear you and they would know the patient's personal details and also that they had mental health issues.

Scenario 10:

The father of an eight-year-old patient pops into the organisation and asks for a copy of the child's vaccination record as they are going travelling for a month in the summer. You know the parents are divorced and the child lives with Mum.

Can you give Dad a copy of the vaccination record?

Parents do not lose parental responsibility if they divorce or separate and you should allow both parents reasonable access to their children's health records. The organisation does not have to seek consent from the other parent and it does not have to tell the other parent that they have received the request.

Note, parental responsibility can be restricted by the courts.

Annex F – Security checklist and risk assessment

UK GDPR SECURITY CHECKLIST AND RISK ASSESSMENT

This organisation has undertaken a security check of the premises and its contents in order to ensure that the organisation has adequate provision to safeguard and protect members of staff, patients, the building and other physical assets, including sensitive and personal information. A series of questions outlined in this annex have resulted in the organisation acknowledging what measures it has in place to mitigate any potential risks / hazards that may arise in the event of any incidents. Each question has had its answer risk assessed using the following criteria:

- **High Risk** – Could have a serious impact on the delivery of patient care, the security of the building, its contents, staff and confidential / sensitive information **(Action required)**

- **Medium Risk** – Some impact on the delivery of patient care, the security of the building, its contents, staff and confidential / sensitive information security **(Action to be considered)**

- **Low Risk** – Short-term disruption to service with low impact on the delivery of patient care, the security of the building, its contents, staff and confidential / sensitive information security **(No action deemed necessary)**

Action plans have been raised within this annex to address any gaps or weaknesses in provision. Staff are aware of the need to report any areas of concern to the Data Protection Officer or IG Lead so that appropriate action can be taken.

Question	State what you have to support your response or why you think it is not necessary / state action plan if appropriate	Risk level H/M/L	If action is required: Person responsible / target date for completion	Completion date
What security measures are in place to safeguard the outside of the building, such as fencing, lockable gates, restricted access?				
Is there any security to monitor the outside of the building such as CCTV, security company surveillance?				
Does the building have an alarm system that is serviced annually and supported by a maintenance contract?				
Does the security system cover all areas of the building – in particular, rooms that contain IT equipment or records?				
Is the security system connected to a Police Station or a Call Response Centre?				
How often is the security alarm code changed?				
Are there warnings on windows, visible alarms, etc. to alert potential intruders that there are physical security measures in place?				
What types of lighting does the building have on the outside and does it adequately protect staff when they enter/leave?				

E.g., security lighting, flood lighting, street lighting.				
How are external doors protected? E.g., five-lever locks or equivalent.				
How are fire and external doors secured? E.g., kept closed when not in use.				
Do all windows have locks that are secured when rooms are not in use?				
How are rooms secured when not in use?				
How is access restricted to the reception and administrative areas of the building?				
What types of security devices are in place to safeguard internal doors to rooms that hold IT equipment / patient records? E.g., keypads, swipe cards, locks.				
What security measures are in place to protect areas where private and confidential information is stored?				
What policy is in place for ensuring that windows, blinds and doors are closed, locked and checked at the end of every working day?				
When the building is not fully occupied, how are unused areas secured?				
What provision does the organisation have for keeping keys safe?				
Is there an agreement in place for				

members of staff or associates who have keys, keypad codes, swipe cards to access the building?				
How often are keypad codes changed?				
Does the organisation have a signing in/out policy for attached staff?				
How does the organisation establish whether visitors (NHS, third-party, etc.) have relevant IG clauses in their contracts of employment?				
Are ID badges worn by staff at all times?				
How does the organisation keep a record of visitors?				
How does the organisation establish whether an appropriate confidentiality agreement has been signed?				
How does the organisation identify visitors on its premises? E.g., visitor badges, work permits.				
Does the organisation have a procedure for challenging unidentified visitors in controlled areas?				
How are deliveries to the organisation supervised? E.g., stationery orders?				
Who is responsible for maintaining the organisation's information asset register? E.g., for hardware, software, manual				

records, services, portable computing equipment.				
How frequently is the asset register reviewed and updated?				
On checking all computer screens and locations, are they angled so that they cannot be viewed by unauthorised personnel from inside and/or outside the building?				
Is all IT equipment asset marked?				
How does the organisation monitor the movement of portable IT equipment used outside the building?				
Where are laptops and other items of portable equipment stored overnight?				
Does the organisation have a protocol for transporting confidential information off-site and, if so, where it can be found?				
Where is the clinical system server located and what safeguards are in place to ensure its security?				
What provision does the organisation have to ensure that the clinical system server is protected by an uninterrupted power supply?				
How is the organisation able to check that the clinical system backup battery is working?				

Is all electrical equipment PAT checked annually?				
Does the organisation have a fireproof safe where backup tapes and other sensitive media or documentation can be kept?				
How many CO^2 fire extinguishers are available within the building and are they regularly serviced by contract?				
How does the organisation manage role-based access to the clinical system for employed and attached staff?				
Are all users of the clinical system given their own unique ID and password?				
How does the organisation ensure that all computer users are aware that passwords should not be divulged or shared?				
How frequently are passwords changed?				
How can you assure that smartcards are used appropriately every time the clinical system is accessed?				
Is it documented that any users of computer systems are required to change user/lock-down or log-out (as appropriate) when leaving their workstation?				
How does the organisation conduct 'audit trails' to check (when necessary) appropriate access of patient information				

by employed/attached staff?				
How long does it take for automatic screen savers to activate?				
Where practicable, does the organisation have a clear screen/clear desk policy and, if so, where can it be found?				
Does the organisation have a documented process to follow for clinical system backups and storage of backup tapes?				
What procedure does the organisation follow to check that backups work?				
Does the organisation have a business continuity plan that covers loss of premises, computer systems, utilities, essential supplies, security systems, paper records, clinical/non-clinical cover?				
How will the business continuity plan be tested for effectiveness?				
Additional notes / comments				

Completed by		**Date completed**		
Next review due				

Annex G – Accountable suppliers register

Supplier name	Contact details	Product / service supplied	Start of contract date	End of contract date

Annex H – Audit template for spot checks

INFORMATION GOVERNANCE SPOT CHECK QUESTIONNAIRE

Location		Date		Auditor	

ICT security

ICT security	Comments	Results
How many PCs are within the public area?		
How many are secured against theft?		
How are they secured against inappropriate access?		
How many of these computers are currently unattended and unlocked?		
How many smartcards have been left in the keyboard at desks which are currently unattended?		
Are screens viewable to the public?		
Random check of C drives for confidential information		
Are any passwords written down or visible?		

How many staff are currently in date with their IG training?		
How many staff are due to undertake their annual IG training in the next month?		

Communication

Communication	Comments	Results
Is the clear desk policy being implemented?		
Is there facility for calls to be taken in privacy?		
Check to see if calls can be heard from the public area		
Is there an answerphone in the public area?		
Is this listened to whilst the public are present?		
Check to see if there is any confidential material left in view		

Physical security

Physical security	Comments	Results

Is access to staff-only areas restricted by a security device?		
Are there any public areas that are closed for any period, e.g., during lunch?		
Is the area secured against entry during these periods?		

Security of confidential information

Security of confidential information	Comments	Results
Is confidential information used in a public area?		
What security is used to protect this information?		
Are locked cabinets available?		
Check the reception area, walls and desks to see if confidential information is clearly on view.		
Within staff-only areas, is confidential information kept secure?		
Can confidential information be seen from outside the area?		

Have information asset owners and information asset administrators been identified and are they aware of their responsibility?		
Have the Information Risk Management Tool and Information Asset Register been updated to take into account the system and information flows?		
Any other observations?		

Records security

Records security	Comments	Results
How are records stored?		
Where are other records stored?		
Where are records archived?		

Disposal of confidential information

Disposal of confidential information	Comments	Results
Is there any shredding stored in boxes?		
Any other additional information?		

NON-COMPLIANCE OBSERVATIONS AND RECOMMENDATIONS

ICT security Details of non-compliance		
Extent of non-compliance	Major □	Minor □
Recommendations		

Communication Details of non-compliance		
Extent of non-compliance	Major □	Minor □
Recommendations		
Physical security		

Details of non-compliance		
Extent of non-compliance	Major □	Minor □
Recommendations		

Security of confidential information Details of non-compliance		
Extent of non-compliance	Major □	Minor □
Recommendations		

Records security Details of non-compliance	

Extent of non-compliance	Major □	Minor □
Recommendations		

Disposal of confidential information Details of non-compliance		
Extent of non-compliance	Major □	Minor □
Recommendations		

Annex I – Example of an audit report template

INFORMATION GOVERNANCE REPORTING FORM

Please use this form to report the details of any actual or potential incidents that affect the confidentiality and security of patient information; it should then be given to the Information Governance Lead for further action.

General information	
Register number (to be added by the IG Lead):	
Reported by:	Date/Time detected:
Title:	Date/Time reported:
Email:	Telephone:
Incident details	
Incident summary (state the facts only: where it occurred, what information was involved, etc.):	

Type of incident *(tick a category)*: ☐ Confidentiality (e.g., breach due to unauthorised access, potential breach due to lost record, etc.) ☐ Integrity (e.g., records altered without authorisation, etc.) ☐ Availability (e.g., records missing, misfiled, theft, etc.)
Impacts on the organisation *(total failure, business as usual, etc.)*:
Type of system(s) affected *(clinical, patient information, finance, administration)*:
What is the information?
What security controls were in place?

Was the information encrypted?	
Scale of incident: how many individuals is the information about?	
Incident details *(state the facts only: where it occurred, what information was involved, what you did, who will you report to/who have you reported to)*:	
Investigation and management	
Name of person investigating:	Date of commencement of investigation:
Investigations, findings, actions and recommendations:	
Post-incident reporting	

Incident and investigation outcome reported to *(add any other relevant notes here, e.g., issue and outcome discussed at staff meeting)*:	ICB YES/NO
	Information Commissioner YES/NO
	Organisation insurer YES/NO
	CQC YES/NO
	Other