****

**Information Governance and Record Keeping Policy**

**[Date of Issue]**

|  |  |
| --- | --- |
| Policy Lead: | [Policy Lead] |
| Version No. | 1 |
| Date of Issue: | [Date of Issue] |
| Date for Review: | [Date of Review] |

CONTENTS

[1. Introduction 3](#_Toc147999902)

[2. Policy Statement 3](#_Toc147999903)

[3. Scope 3](#_Toc147999904)

[4. Definitions 4](#_Toc147999905)

[5. Personal Data Audits 4](#_Toc147999906)

[6. Information Asset Register 5](#_Toc147999907)

[7. Access to Information and Disclosure Outside of [Company Name] 6](#_Toc147999908)

[8. Individual Awareness 6](#_Toc147999909)

[9. Security Breach Notification and Investigation 6](#_Toc147999910)

[10. Individual Rights 7](#_Toc147999911)

[11. Fair and Lawful Procedures 12](#_Toc147999912)

[12. Retention of Information 13](#_Toc147999913)

[13. Responsibilities in the Event that [Company Name] Ceases Trading 16](#_Toc147999914)

[14. Data Quality 17](#_Toc147999915)

[15. Disclosing Personal Data 17](#_Toc147999916)

[16. Information Security 20](#_Toc147999917)

[17. Freedom of Information 27](#_Toc147999918)

[18. Roles and Responsibilities 28](#_Toc147999919)

[19. Monitoring and Compliance of the Policy 29](#_Toc147999920)

[20. Related Policies 29](#_Toc147999921)

[21. Legislation and Guidance 29](#_Toc147999922)

[22. Summary of Review 30](#_Toc147999923)

# Introduction

Information Governance gives assurance to data subjects, including members of staff, individuals and clients that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care. [Company Name] recognises that it is of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

# Policy Statement

All members of staff must comply with this policy. In order to discharge its requirements, [Company Name] must ensure that clear policies and procedures are in place and that they are supported by effective awareness training. It is [Company Name]’s policy that personal data will be:

* obtained, held and processed fairly
* held for specific purposes and used only for these purposes
* processed in accordance with the rights of the data subject
* relevant, accurate and kept up to date
* corrected if shown to be inaccurate
* kept for no longer than necessary and destroyed when no longer required, in line with best practice
* protected against loss or unauthorised or unlawful processing, accidental loss and destruction or damage using appropriate technical or organisational measures.

This policy should be read in conjunction with the Confidentiality Policy.

# Scope

This policy applies to all members of staff at [Company Name] who should ensure that they are aware of their responsibilities in relation to information governance.

This policy applies to all personal data processed by [Company Name] relatable to any identifiable living person.

# Definitions

**Data subject:** the individual about whom [Company Name] has collected personal data.

**Data Protection Act 2018:** an Act of Parliament that updates data protection laws in the UK. Following UK departure from the European Union, DPA 2018 continues to apply and provisions of the EU GDPR were incorporated directly into UK law. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

**Personal data:** any information about a living person including, but not limited to, names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, as defined below.

**Process or processing:** doing anything with personal data, including, but not limited to, collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data; at the point you collect it, you are processing it.

**Special categories of data** have an equivalent meaning to ‘sensitive personal data’ under the Data Protection Act 2018. Special categories of data include, but are not limited to, medical and health records (including information collected as a result of providing health care services) and information about a person’s religious beliefs, ethnic origin and race, sexual orientation and political views.

**Data controller:** the main decision-maker over the management of the data in question. They exercise overall control over the purposes and means of the processing of personal data. For the purposes of this policy, [Company Name] considers itself to be a data controller in respect of all members of staff and clients.

**Data processor:** acts on behalf of and only on the instructions of the relevant controller. For the purposes of this policy [Company Name] considers that they are the data processor in relation to the service delivered to its clients.

# Personal Data Audits

[Company Name] will carry out PID (Personally Identifiable Data) Audits. The data audit will be carried out by the Data Protection Officer **[Keep this term if a qualified Data Protection Officer otherwise change to Data Protection Lead]** or a person to whom the Data Protection Officer/Data Protection Lead has delegated this task responsibility and the results collated. The personal data audit will identify the following:

* whom the information is held about
* what personal information is held, including any sensitive personal data
* in which format the personal data is being collected (e.g., name, address, telephone number etc.)
* how the PID is stored (e.g., on a computer, manual files or both)
* who has access to this information
* the purpose(s) for which [Company Name] holds the personal data
* how the PID is collected
* whom the PID is collected from.

**[This paragraph is for larger companies only. All large companies must have a Data Protection Officer. Delete this paragraph if you’re a small company]** A Personal Data Audit form is available from the Data Protection Officer, [Data Protection Officer Name]. The Data Protection Officer will use the outcome of the Personal Data Audit to update the Information Asset Register.

**[For smaller companies who do not have a designated Data Protection Officer]** A Personal Data Audit form is available from The Registered Manager. The Registered Manager will use the outcome of the Personal Data Audit to update the Information Asset Register.

# Information Asset Register

Computerised and manual filing systems containing information relating to an identifiable person who can be directly or indirectly identified, such as name, identification number, location data or online identifier, must be documented in the Information Asset Register. The Asset Register will record:

* the Service Area to which the entry relates
* the name of the computer system, manual files or both in which the data is stored
* whom the information is held about
* what personal information is held, including any sensitive personal data that is being held
* how the data is protected (e.g., restricted access or protected access)
* retention period for the data
* The Information Asset Owner

Such systems must be managed to comply with GDPR/Data Protection principles.

# Access to Information and Disclosure Outside of [Company Name]

Members of staff will be granted access to the information that they need to carry out their work. Members of staff have a duty to keep the information they use confidential.

There are a number of occasions where it will be necessary for [Company Name] to share PID. The correct parameters of when it is appropriate to share and disclose data include relevant agreements and protocols that are in place that allow for the exchange of information between [Company Name] and other organisations. Any information disclosed must be necessary for the purpose for which it is disclosed. Therefore, members of staff should not, for example, disclose details of a member of staff’s religious beliefs if only their name and National Insurance number is required by the HMRC.

If it is necessary to discuss individual data subjects in reports or at meetings, a pseudonymisation process should be followed (e.g., Nurse A).

# Individual Awareness

It is [Company Name]’s policy that:

* Information Governance training will be classified as ‘mandatory’ in the induction programme
* all new members of staff to the business will receive information governance training relevant to their role, as soon as possible on commencement of their employment
* all individuals associated with [Company Name]. whether employed or contracted, will receive information governance training at least every 12 months
* guidance and support is available to all members of staff who process PID.

# Security Breach Notification and Investigation

Any breach or suspected breach of the GDPR must be reported immediately to the Data Protection Officer/Data Protection Lead, providing as much information as possible. A breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability or personal data. There will be a personal data breach whenever personal data is lost, destroyed, corrupted or disclosed, as well as if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable, for example, when it has been encrypted by ransomware or accidentally lost or destroyed.

The Data Protection Officer/Data Protection Lead will investigate and, if appropriate, produce a report for the Senior Management Team. The Data Protection Officer/Data Protection Lead will provide advice to the Senior Management Team on whether the breach requires notification to the Information Commissioner’s Office. This advice should take account of the information provided on the ICO’s website regarding the reporting of breaches.

The Data Protection Officer/Data Protection Lead is required to notify the ICO of any breach that is likely to present a risk to the rights and freedoms of data subjects. If a decision is made not to report a breach to the ICO, the rationale must be documented so that it can be justified at a later date if required.

[Company Name] will ensure a record is kept of all data breaches as well as details of lessons learned. These will be shared throughout [Company Name] in line with the Incident Management Policy as well as themes and trends identified and acted upon.

# Individual Rights

**The Right to be Informed**

[Company Name]’s privacy notice supplied to clients and members of staff regarding the processing of their personal data will be written in a clear, plain language, which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

* the identity and contact details of [Company Name] and the Data Protection Officer/Data Protection Lead
* the purpose of and the legal basis for processing the data
* the legitimate interest of [Company Name] (if applicable) or a third party
* any recipient categories of recipients of the personal data
* any international transfers of data
* how long the data will be stored for
* the existence of the data subject’s rights, including the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

The privacy notice should also refer to any online information collated such as cookies. In relation to cookies, [Company Name] will:

* tell people the cookies are there
* explain what the cookies are doing and why
* get the person’s consent to store a cookie on their device.

Fresh consent if may be required if the use of cookies changes over time.

**Subject Access Requests (SARS)**

Individuals have the right to obtain confirmation that their data is being processed. They also have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The GDPR requires that the data subject is provided with access to their personal data within 1 month of their request being validated by [Company Name]. [Company Name] may extend the period of compliance by a further 2 months, where requests are complex or numerous. If this is the case, [Company Name] will inform the individual within 1 month of receipt of the request and explain why the extension is necessary.

[Company Name] will verify the identity of the person making the request before any information is supplied. The Data Protection Officer/Data Protection Lead must be advised of all subject access requests and keep a record of these to demonstrate compliance with the requirements of the legislation. The response time will not commence until all of the conditions identified above been satisfied. All requests will be responded to without delay and at the latest, within 1 month of receipt.

A copy of the information will be supplied to the individual free of charge. However, [Company Name] may impose a ‘’reasonable fee‟ to comply with requests for further copies of the same information. Fees will be based on the administrative cost of providing this information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will also be charged.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. All manual data in relevant filing systems will be reviewed and any personal data relating to third parties removed, anonymised or consent for its disclosure obtained from the third party.

Where a request is manifestly unfounded or excessive, [Company Name] holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority (the Information Commissioner’s Office) within 1 month of the refusal.

In the event that a large quantity of information is being processed about an individual, [Company Name] will ask the individual to specify the information the request is in relation to.

**Right to Rectification**

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, [Company Name] will inform them of the rectification, where possible. Where appropriate, [Company Name] will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within 1 month; this will be extended by 2 months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, [Company Name] will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

**The Right to Erasure**

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

* where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
* when the individual withdraws their consent
* when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
* the personal data was unlawfully processed
* the personal data is required to be erased in order to comply with a legal obligation
* the personal data is processed in relation to the offer of information society services to a child.

[Company Name] has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

* to exercise the right of freedom of expression and information
* to comply with a legal obligation for the performance of a public interest task or exercise of official authority
* for public health purposes in the public interest
* for archiving purposes in the public interest, scientific research, historical research or statistical purposes
* the exercise or defence of legal claims.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, [Company Name] will inform the other organisations who process the personal data to erase links to and copies of the personal data in question.

**The Right to Restrict Processing**

Individuals have the right to block or suppress the processing of personal data by [Company Name].

In the event that processing is restricted, [Company Name] will store the personal data, but will not process it further, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. [Company Name] will restrict the processing of personal data in the following circumstances:

* where an individual has objected to the processing and [Company Name] is considering whether there are legitimate grounds to override those of the individual
* where processing is unlawful and the individual opposes erasure and requests restriction instead
* where [Company Name] no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Where an individual contests the accuracy of the personal data, processing will be restricted until [Company Name] has verified the accuracy of the data. If the personal data in question has been disclosed to third parties, [Company Name] will inform them about the restriction on the processing of the personal data, unless it is impossible or involves a disproportionate effort to do so. [Company Name] will inform individuals when a restriction on processing has been lifted.

**The Right to Data Portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

* to personal data that an individual has provided to a controller
* where the processing is based on the individual’s consent or for the performance of a contract
* when processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form. The information will be provided free of charge. [Company Name] is not required to adopt or maintain processing systems that are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, [Company Name] will consider whether providing the information would prejudice the rights of any other individual.

[Company Name] will respond to any requests for portability within 1 month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by 2 months, ensuring that the individual is informed of the extension and the reasoning behind it within 1 month of receipt of the request.

Where no action is being taken in response to a request, [Company Name] will, without delay and at the latest within 1 month, explain to the individual the reason for this and will inform them of their right to complain to the Information Commissioner’s Office.

# Fair and Lawful Procedures

Under the GDPR, data will be lawfully processed by [Company Name] under the following conditions:

* the consent of the data subject has been obtained
* processing is necessary for:
  + compliance with a legal obligation
  + the performance of a task carried out in public interest or in the exercise of official authority vested in the controller
  + for the performance of a contract with the data subject or to take steps to enter into a contract
  + protecting the vital interests of a data subject or another person
  + for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

* [Company Name] will not use personal data for any purposes other than those advised to individuals directly or detailed in the relevant entry in the Register of Data Controllers published by the Information Commissioner’s Office
* as far as possible, [Company Name] will process personal data only where it is necessary for compliance with the law, the performance of a contract, with a view to establishing a contract, or it is in the organisation’s legitimate business interests to do so
* where this is not possible, or in the case of sensitive personal data (see below), consent of the individual will be sought to enable the personal data to be processed.

[Company Name] will obtain the explicit consent of the individual concerned for all processing of sensitive personal data, unless:

* it is information relating to racial/ethnic origin, disability or religious belief that is being collected purely for monitoring equality of opportunity or treatment
* it relates to the employment of individuals
* it is necessary for the provision of advice or support and the data subject cannot reasonably be expected to give explicit consent.

[Company Name] will require all data processors to formally agree that personal data will not be used for any purpose other than that agreed. [Company Name] will not disclose personal data to third parties, unless:

* carrying out obligations under employment, social security or social protection law or a collective agreement
* protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
* the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
* reasons of substantial public interest on the basis of Union or Member State law, which is proportionate to the aim pursued and which contains appropriate safeguards
* the purposes of preventative or occupational medicine, for assessing the working capacity of the members of staff, medical diagnosis, the provision of health, social care, treatment, management of health, or social care systems and services on the basis of Union or Member State law or a contract with a health professional
* reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
* archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

All disclosures of personal data to third parties must be authorised by a member of the Senior Management Team and be limited to the minimum information required. All disclosures must be recorded either in the personnel or client ’s record.

# Retention of Information

Personal data shall be retained in accordance with the period detailed below. Where a retention period is not specified, personal information will only be retained for the longer of:

* as long as required for its purpose
* as required by law
* as recommended by the Chartered Institute of Personnel & Development.

Paper based records will be disposed of in the confidential waste bins provided ready for shredding. Further advice can be sought from the Data Protection Officer/Data Protection Lead. [Company Name] requires all data processors to formally agree that personal data shall not be retained for longer than the purpose for which they are processing it. In the table below, retention periods in bold are statutory, those not in bold are best practice:

| **Record** | **Retention** | **Comment** |
| --- | --- | --- |
| Application forms of non-short-listed candidates | **6 months** | Equality Act 2010 |
| Short lists, interview notes and related application forms | 6 months | Chartered Institute of Personnel and Development recommendation |
| Personnel records (incl. training & disciplinary) | 6 years after employment ceases | Chartered Institute of Personnel & Development recommendation |
| Redundancy details/ calculations | 6 years after redundancy | Chartered Institute of Personnel & Development recommendation |
| Wage/salary/payment records | **6 years** | Taxes Management Act 1970 |
| SMP & SSP records (incl. certificates & self-certification) | **3 years after end of related tax year** | SMP Regulations  SSP Regulations |
| Parental leave | 5 years from birth/adoption | Chartered Institute of Personnel & Development recommendation |
| Incident details | 10 years after incident | NHS England Records Management Code of Practice 2023 |
| Serious incident details (including RIDDOR reportable incidents) | 10 years after incident | NHS England Records Management Code of Practice 2023 |
| [Company Name]’s members of staff (incl. training / contact information / PID) | Records of significant training and staff details must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member’s role. The following is recommended: statutory and mandatory training records - to be kept for ten years after training completed other training records - keep for six years after training completed | NHS England Records Management Code of Practice 2023 |

Healthcare records must be retained in line with the Private and Voluntary Health Care (England) Regulations 2001 as outlined below:

|  |  |
| --- | --- |
| **Type of Patient** | **Minimum Period of Retention** |
| Patient who was under the age of 17 at the date on which the treatment to which the records refer was concluded | Until the patient’s 25th birthday. |
| Patient who was aged 17 at the date on which the treatment to which the records refer was concluded. | Until the patient’s 26th birthday. |
| Patient who died before attaining the age of 18. | A period of 8 years beginning on the date of the patient’s death. |
| Patient who was treated for mental disorder during the period to which the records refer | A period of 20 years beginning on the date of the last entry in the record. |
| Patient who was treated for mental disorder during the period to which the records refer and who died whilst receiving that treatment. | A period of 8 years beginning on the date of the patient’s death. |
| Patient whose records relate to treatment by a general practitioner. | A period of 10 years beginning on the date of the last entry. |
| Patient who has received an organ transplant. | A period of 11 years beginning on the date of the patient’s death or discharge whichever is the earlier. |
| All other cases. | A period of 8 years beginning on the date of the last entry in the record. |

Methods used for disposal of confidential information must continue to protect confidentiality. Paper information should be shredded by means of the paper shredding service using the secure, locked consoles placed at various sites within [Company Name]. When data needs to be permanently deleted from IT systems, advice will be sought at the time from an ISO accredited IT specialist on the best method to ensure this is permanently and completely removed from any systems.

All redundant, faulty or obsolete removable storage media, such as external hard drives which did or which may have contained sensitive or valuable information during their life cycle, should be returned to the IT team to ensure complete removal of information/information storage capability.

# Responsibilities in the Event that [Company Name] Ceases Trading

In the event that [Company Name] is sold to another business, the data relating to our clients will be transferred to the purchasing organisation. [Company Name] will notify all of its data subjects of the fact that the data is being transferred and that the purchaser will be the data controller from the date of completion of the purchase.

In the event that [Company Name] ceases trading altogether, records will be managed in line with the guidelines contained NHS England Records Management Code of Practice 2023 and retained in accordance with the retention schedule above.

In practice, if the business is liquidated or goes into administration, it is likely that the liquidator or administrator becomes the new most senior member of staff, and they will take over all key decisions.

As a care organisation, [Company Name] will still have a legal obligation to continue holding data for a length of time, and as such the business will continue to be the controller of that personal data and data protection laws still apply.

This includes continuing registration with the ICO.

# Data Quality

All forms used to collect personal data shall only ask for information that is relevant to the purpose of the form. At least once each year, members of staff and clients will be provided with an opportunity to confirm the accuracy of any personal data held on [Company Name]’s IT systems.

Changes in personal data relating clients or members of staff must be promptly and accurately updated on the appropriate computer system(s).

All notes recorded will be saved on the personnel file. The information must be accurate and relevant and not express any subjective opinion relating to an individual’s personal characteristics.

# Disclosing Personal Data

All personal data will be protected from unauthorised access by appropriate organisational and technical security measures. Personal data will not be disclosed to data processors unless there is a contract or confidentiality agreement in place, which defines the authorised use(s) to which the data can be put. Personal data will not be disclosed to the data subject via a telephone where the authenticity of the requestor cannot be reliably established.

Personal data disclosed to the data subject in response to a Subject Access Request must be reviewed before disclosure to ensure that it does not include any information that infringes the rights and freedoms of any third party or is exempt from disclosure.

Personal data will not be disclosed to third parties where the identity of the third party cannot be reliably established. Personal data will only be disclosed to third parties when **one** of the following conditions is met:

* the data subject has given [Company Name] their consent to disclose the information (including where there is a Lasting Power of Attorney)
* disclosure is essential to the lawful purpose for which the personal data is being processed
* the data subject has given the third party their consent to request the information
* the disclosure is subject to a formal Information Sharing Protocol and is made within the terms of that protocol
* disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)
* disclosure is in the vital interest of the data subject.

Sensitive personal data will only be disclosed to third parties when **one** of the following conditions is met:

* the data subject has given their explicit consent for the disclosure or a best interest decision has been made – see Mental Capacity Act and DoLS Policy
* the data subject has given the third party their explicit consent to request the information
* disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)
* disclosure is in the vital interest of the data subject.

Disclosure in respect of the last two conditions of this policy must not be made without the formal authorisation of the Data Protection Officer/Data Protection Lead. All disclosures of personal data to data processors and third parties will be limited to the minimum information required to satisfy the requirements of the contract or legitimate request.

Consent must be obtained before an individual’s personal data is published in any [Company Name] publication. In the case of sensitive personal data, the consent must be explicit (e.g., signing of the pre-publication article).

The disclosure of personal data must be recorded in an appropriate IT system.

**Factors to consider**

When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) you should consider what the sharing is meant to achieve? There should be a clear objective or set of objectives. Being clear about this will identify the following:

* Could the objective be achieved without sharing the data or by anonymising it? It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.
* What information needs to be shared? You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies “Use the minimum necessary personal confidential data “.
* Who requires access to the shared personal data? You should employ ‘need to know’ principles, meaning that when sharing both internally between departments and externally with other organisations, individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.
* When should it be shared? Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
* How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
* How can we check the sharing is achieving its objectives? You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.
* How are individuals made aware of the information sharing? Have individuals been provided with the fair processing information as required by the GDPR? How is it ensured that individual’s rights are respected and can be exercised e.g. how can they access the information held once shared?
* What risk to the individual and/or the organisation does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals’ trust in the organisations that keep records about them?
* What is the legal basis for data protection purposes? Organisations must identify the lawful basis (e.g. meeting statutory duties) for processing and, where necessary, a condition for processing special categories data (e.g. managing a health and care service).
* If the information is confidential, what is the legal basis that complies with the common law duty of confidence? This can be consent (implied or explicit), overriding public interest or required or permitted by law. It is good practice to document all decisions and reasoning related to the information sharing.

It is good practice to document all decisions and reasoning related to the information sharing.

**Secondary Uses of Data**

A secondary use of data is where PID is used for work not directly related to the care of the patient and when information is processed for non-healthcare and medical purposes.

Generally, this could be for research purposes, audits, service management, commissioning, performance management, capacity planning, service redesign and benchmarking, contract monitoring and reporting facilities. [Company Name] may use data for secondary purposes from time to time but will always ensure that the data is pseudonymised when not being used for direct-care purposes.

# Information Security

[Company Name] has a systematic approach to information security risk management and identifies business needs regarding information security requirements (including contractual and regulatory). During the delivery and maintenance of [Company Name]’s services, there are a number of instances where risk assessment is necessary (e.g., disclosure to third parties).

The following actions serve as effective risk mitigations when it comes to securing data:

* a practical, clear desk policy so that no personal or sensitive information or information of a confidential nature is left on unattended desks or in offices in such a way that it could be accessible to any person who is not authorised to have such access
* information assets and information processing facilities are protected against unauthorised access
* information is protected from unauthorised disclosure
* confidential and sensitive information is appropriately classified as such
* appropriate arrangements are in place to encrypt laptops and emails containing personal information
* appropriate arrangements are in place to manage the uploading and downloading of confidential and sensitive information from IT equipment
* unsupported systems (including software, hardware and applications) should be identified and a plan put in place to remove, replace or actively mitigate or manage the risks associated with any unsupported system
* confidentiality of information assets is a high priority
* integrity of information will be maintained
* [Company Name] requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities are met
* statutory, expressed and implied legal obligations are met
* business continuity plans shall be produced, maintained and tested.

Access to system, data or networks should be granted only to users that have formally agreed to comply with [Company Name]’s Information Governance Policy which details how information should be handled and protected. This will be achieved through appropriate clauses in staff and contractor contracts and through the completion of mandatory IG training. Unauthorised and illegal use of information assets and information processing facilities is prohibited. Use of non- [Company Name] approved web-applications (such as cloud services) to process confidential information is not permitted without this being approved for use by the Senior Leadership Team. The use of obscene, racist or otherwise offensive statements shall be dealt with in accordance with other policies published by [Company Name].

This policy is communicated to all individuals working with [Company Name] for whom information governance training shall be given. All breaches of information security, actual or suspected, must be reported and investigated in line with [Company Name] policies. Controls are commensurate with the risks faced by [Company Name].

**White Boards**

Any PID should not be displayed in an office on a white board where members of the public can view or see from the exterior of the building. Backgrounds should be particularly borne in mind when using video-conferencing facilities.

**Computers**

PID must only be stored on Company equipment and not on personally owned laptops or home desktop computers.

IT assets should have a named information asset owner, responsible for the information security of that asset. The Information Asset Register should be maintained by the IT team. All new information systems must be designed to consider information security and data protection requirements and the management of computers and networks should be controlled through documented procedures. The Information Asset Owner is responsible for ensuring the security of data stored in the named system.

Any changes to information systems, applications or networks should be reviewed and approved in accordance with a documented change management process. Similarly, all information products must be properly licensed and technical controls should ensure that users cannot install software on the company’s property. Software countermeasures and management procedures must be used to protect against the threat of malicious software.

All files containing personal identifiable information, held on Company owned computer equipment should be "encrypted/password" protected, and preferably not held by the data subject’s name, substituting a suitable identifier other than name. Particular care should be taken with portable devices. The ideal is that portable devices should only act as terminals to the main networked system since the data is then protected in the Company network.

Personal identifiable data should not be kept on the hard drives of PCs unless formally justified by the Data Protection Officer/Data Protection Lead, due to the risk of theft and breach of confidentiality. Such files should be stored on the network, where they will be backed up centrally by the IT team.

Files containing individual person-identifiable information on portable computers should be password protected, or better still not stored on a portable device. Files stored on network drives do not require password protecting, as a password is needed to log on to the network and access to folders is restricted.

Users should not leave terminals logged in and unattended. Screens should be locked as soon as the user moves away from the screen to reduce the risk of unauthorised access to information. Computers should not be transferred between users or disposed of, other than through the IT team as they have the means of transferring or removing all data from the hard drive.

Certain areas within the company have a requirement to have access to information whilst on the move, whether that is by use of a laptop, tablet, handheld computer, mobile phone or a combination of these. This mobile access creates potential risks to the confidentiality, integrity and availability of the data we hold on behalf of clients and staff members. This policy sets out how mobile computing is to be used within the company to manage the risk to that data. It also balances the need for easy access to information with our responsibility to the individual to ensure we treat their data properly.

Users of portable computers are to ensure that their device is logged onto the network on a regular basis in order to receive regular updates to software and anti-virus signature files. If a virus is discovered it should be immediately reported to the IT team and the device and any media used with it, quarantined immediately for inspection and cleaning.

Users issued with a [Company Name] owned mobile device will be connected to their email and calendar functions by use of the Company’s selected Mobile Device Management (MDM) software solution. The MDM software ensures security of the company data, and, that there is no interaction between the company data and the remainder of the device.

Users are forbidden from attempting to ‘jailbreak’ the device or otherwise attempt to alter its security configuration. Users are also forbidden from downloading and installing applications without prior approval from IT.

**(Delete if you do not have an IT team)** [Company Name] and its Information Technology (IT) Team shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the company’s property without permission from the IT team. Users breaching this requirement may be subject to disciplinary action.

As working practices change and staff members become more mobile there is now a need for users to access their email, calendar and working documents from outside of the normal office environment.

**(Delete if not applicable)** Where there is a requirement for a user to work away from company premises, remote connectivity is only to be used via the company Virtual Private Network (VPN). Use of the company VPN system requires that users are issued with the relevant software and login credentials

It is a user’s responsibility to ensure that their credentials are kept safely and securely. Credentials must be kept confidential and not disclosed to anyone. Secure VPN Access can be requested from the IT Team.

**Telephones**

All possible steps must be taken to ensure that information regarding an individual is not divulged over the telephone to anyone without authority. Asking for key details about the individual (e.g., date of birth) may not be sufficient to ensure that the caller has a need to know.

Where there is any doubt regarding the identity of the person requesting the information, guidance should be sought from the Data Protection Officer/Data Protection Lead. If advice is not immediately available, then the information should not be disclosed. If the caller is claiming to be from an organisation (e.g., the NMC) then the switchboard telephone number should be obtained (rather than direct line), checked and then used to ensure that the caller is from the agency stated.

A record should be kept of all telephone discussions where information is shared verbally on the personnel file.

**Email**

Personal email addresses should never be used for work purposes. Personal identifiable information must only be sent by e-mail within [Company Name] when attached to a password protected document, spreadsheet or database. Inclusion within the main body of the e-mail is not permitted. The password should be delivered to the intended recipient by a different medium, such as a telephone call or text message.

Personal identifiable information must only be sent externally using an encrypted email. Steps must be taken to ensure that any confidential/sensitive information is sent to the mailbox of the person or persons who are authorised to see that information, and that no unauthorised persons have access to that mailbox/those mailboxes.

Before sending or receiving confidential/sensitive emails, confirm the email address with the other party, spelling any words that may cause errors. Use must be made of the e-mail “Tracking Options” where available, to notify that a message has been delivered and/or read. Otherwise, the sender must be telephoned to confirm receipt. A copy of the e-mail and its attached documents must be stored appropriately within manual and/or electronic records, and the original email deleted from both the inbox and deleted items.

All members of staff should be mindful of using the ‘reply all’ and ‘cc’ buttons to prevent against other people receiving information unnecessarily. There must be a justified reason for anyone to be copied into or sent PID.

**Video Conferencing**

Prior to utilising any video conferencing (or otherwise) software a Data Protection Impact Assessment should be carried out to determine the implications of using the new technology on the privacy rights of individuals.

Privacy settings of all software in particular should be examined thoroughly to determine their adequacy. The rights of data subjects should also be kept in mind when choosing a software service (e.g., the ease in which chat data can be extracted which may relate to an individual).

Members of staff should also be mindful of their backgrounds when using video conferencing facilities and ensure that no identifiable information is visible behind them.

It is also important to be aware that there may be other people within the room that cannot be seen on screen or are within earshot and as such confidential or private information should not be disclosed as a matter of course, without first checking with the individual whether they agree to this.

Video conference chats should not normally be recorded without obtaining the consent of the individual involved and if this is done, the privacy notice should be updated to reflect this.

**Third Parties**

The risks associated with engaging a third party will be identified, assessed and managed and due diligence shall be undertaken in any such proposals. Where third parties are used to manage information or information processing facilities, a formal contract shall be in place that defines the information security requirements of the relationship.

The delivery of the contracted services is monitored, and formal procedures are in place to manage change and the identification, reporting and management of information security incidents. Contracts with third parties shall provide [Company Name] with the right to audit the third party. All contracts with third parties that will process data on behalf of [Company Name] will contain the relevant contractual clauses outlined within the GDPR.

**Privacy by Design and Privacy Impact Assessments (DPIA)**

[Company Name] will act in accordance with the GDPR by adopting a privacy by design approach, which will seek to ensure that [Company Name] have considered and integrated data protection into processing activities where required.

The GDPR does not require a DPIA to be carried out for every processing operation that may result in risks to the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where a processing is “likely to result in a high risk to the rights and freedoms of natural persons”. It is particularly relevant when a new data processing technology is being introduced.

DPIAs will be used to identify the most effective method of complying with [Company Name]’s data protection obligations when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. High risk processing includes, but is not limited to, the following:

* a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
* processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences
* systematic monitoring of a publicly accessible area on a large scale.

In risk management terms, a DPIA aims to manage risks to the rights and freedoms of natural persons, using the following three processes, by:

* establishing the context: considering the nature, scope, context and purposes of the processing and the sources of the risk
* assessing the risks: assess the particular likelihood and severity of the high risk
* treating the risks: mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

[Company Name] will seek to ensure that all DPIAs include the following information:

* a description of the processing operations and the purposes
* an assessment of the necessity and proportionality of the processing in relation to the purpose
* an outline of the risks to individuals
* the measures implemented in order to address risk.

**Client Confidentiality**

For further information specifically relating to client confidentiality, please refer to the Client Confidentiality Policy.

**Record Keeping**

The principles of effective record keeping are:

* Accessible to all staff that require access in order to enable them to carry out their duties – information must be stored in the correct areas on the system and are entered via approved data entry formats where they exist.
* Understandable, clear and concise – Records must avoid the use of jargon and technical terminology as the client must be able to read and understand what is written about them. The record may also be accessed by other professionals for the purposes of care delivery and they must be able to understand what is written. Abbreviations should not be used within the care record. Where a staff member wishes to abbreviate anything, this should be written in full in the first instance with the abbreviation written in brackets after.
* Factually accurate and relevant – Records must be a factual record of the care that is delivered and where possible, collateral evidence should be sought. The record must not contain irrelevant information or personal opinions.
* Secure – Passwords and PIN numbers should not be written down or shared, and if working on non-Company premises, staff must ensure that their computer screens cannot be seen by others. Paper records should only be used in the event of system failure and these should be scanned onto the EPR once the system is live. The purpose of a care record is to facilitate the care, treatment and support of a particular client. In order to ensure that records are created in a consistent and professional manner the Records management: code of practice for health and social care (2021) should be adhered to at all times.

# Freedom of Information

[Company Name] is only required to provide information under the Freedom of Information Act 2000 in respect of the activities that it carries out whilst under contract with a public authority. As such, [Company Name] is not required to respond to FOI requests received directly from members of the public in relation to any other of its commercial activities. If such a request is received, the Registered Manager should refer the requesting party to the scope of the legislation and politely decline to provide the information.

Upon receipt of an FOI request, the Registered Manager will endeavour to ensure that the requested information is collated and returned to the contracting public authority to allow them to meet the 20-working day deadline of the legislation. Prior to sending any information it should be checked for any personal data, which should be redacted prior to sending.

In certain circumstances [Company Name] may be asked for our views as to whether certain information should be released before the public body decides as to how to respond. The person responsible for making this decision in [Company Name] would be the Registered Manager.

If [Company Name] provides any information to a public body on the understanding that it is confidential, this should be highlighted on the documents provided. If information has not been provided to a public body on a confidential basis, the public body may consult with [Company Name] as to whether any exemptions under the legislation may apply (for example prejudicing commercial interests).

# Roles and Responsibilities

The Data Protection Officer/Data Protection Lead has overall responsibility for information governance within [Company Name]. The Data Protection Officer/Data Protection Lead is responsible for:

* informing and advising [Company Name] and individuals associated with the business about their obligations to comply with the GDPR and relevant data protection legislation
* monitoring compliance with the GDPR and other data protection legislation, including managing internal data protection activities and ensuring that relevant training is available for all members of staff
* acting as the first point of contact for regulatory authorities and for data subjects
* investigating any breaches of the GDPR, reporting such breaches as appropriate and ensuring that appropriate arrangements are put in place to prevent similar breaches occurring in the future.

The Registered Manager is responsible for:

* carrying out and keeping up to date a personal data audit
* ensuring that this policy is implemented within their team and that all members of staff receive Information Governance Training in line with this Policy.

# Monitoring and Compliance of the Policy

The Data Protection Officer/Data Protection Lead is responsible for ensuring the ongoing relevance of this Policy and for monitoring the consistency of its application. This will primarily be done via face-to-face supervision sessions.

This policy will be routinely reviewed annually by the Data Protection Officer/Data Protection Lead, or earlier if there are any changes in legislation.

# Related Policies

* Confidentiality Policy
* Governance and Risk Policy
* Quality Assurance Policy

# Legislation and Guidance

**Relevant Legislation**

* Data Protection Act 2018
* Freedom of Information Act 2000
* General Data Protection Regulation 2016
* Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003
* Private and Voluntary Health Care (England) Regulations 2001

**Guidance**

* Information Commissioner’s Office Guide to the General Data Protection Regulation: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
* The Information Governance Review: Information to Share or not to Share: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf>
* NHS England Information Security Policy: [information-security-policy-v4.0.pdf (england.nhs.uk)](https://www.england.nhs.uk/wp-content/uploads/2016/12/information-security-policy-v4.0.pdf)
* NHS England Records Management Code of Practice 2023: <https://transform.england.nhs.uk/information-governance/guidance/records-management-code/>

# Summary of Review

|  |  |
| --- | --- |
| Version | 1 |
| Last amended | [Date of Issue] |
| Reason for Review |  |
| Were changes made? |  |
| Summary of changes |  |
| Target audience | Care staff, Managers |
| Next Review Date | [Date of Review] |