Superior Healthcare Group

GDPR Compliance Policy and Procedure

Version 5.0

Contents

Version Control

Document Title	GDPR Compliance Policy and Procedure
Author	Jo Rychlik
Last reviewed	25/04/2024
Next review due	25/04/2025

Version Details

Date	Version No	Status	Author	Reviewer	Approved By	Comments
27/11/2019	1.0	Final	JR	ST	ST	Final for publication
04/12/2020	2.0	Final	JR	ST	ST	Reviewed
03/12/2021	3.0	Final	JR	ST	ST	Reviewed
03/12/2022	4.0	Final	JR	ST	ST	Reviewed
03/12/2023	5.0	Final	JR	ST	ST	Final for publication
25/04/2024	5.0	Final	JR	MP	MP	Reviewed

GDPR Compliance Policy and Procedure

Last reviewed: 25/04/2024

1. Background

- The Superior Healthcare Group makes use of a variety of data about identifiable individuals, including data about:
    - Current, past and prospective employees
    - Customers/clients
    - Users of its websites
    - Subscribers / potential customers
    - Respondents to market research / social research and consultancy-related research
    - Other stakeholders
- Personally Identifiable data (PID) is any data that is specific to an individual and could be used to identify them. For example, their name, address and other contact details, age, salary, religion, health information, or bank details. All of this personal data, stored in any location, must be carefully controlled.
- In collecting and using this data, we are subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

2. Purpose

- To set out the relevant legislation and to describe the steps The Superior Healthcare Group is taking to ensure that it complies with it.
- To set out the steps that need to be taken to ensure that The Superior Healthcare Group handles, uses and processes personal data in a way that meets the requirements of GDPR. It should be read alongside the suite of The Superior Healthcare Group GDPR policies, procedures and guidance.
- To support The Superior Healthcare Group to meet the following Key Lines of Enquiry:

Key Question	Key Line of Enquiry (KLOE)
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?
WELL-LED	W3: How are the people who use the service, the public and employees engaged and involved?

- To meet the legal requirements of the regulated activities that The Superior Healthcare Group is registered to provide:
    - The Data Protection Act 2018
    - The General Data Protection Regulation 2016 (EU) 2016/679
    - Mental Capacity Act 2005
    - Mental Capacity Act Code of Practice

- Records Management Code of Practice for Health and Social Care 2016.

3. Scope

- The following roles may be affected by this policy:
  - All roles.
- The following people may be affected by this policy:
  - Clients ad Prospective Clients, employees (current and former) and Job Applicants, Management Teams, Board Members, Directors, Suppliers, Third Parties who have access to the Superior Healthcare Group systems and/or data.
- The following stakeholders may be affected by this policy:
  - Suppliers
  - Commissioners
  - Family
  - Advocates
  - Representatives
  - Commissioners
  - External health professionals
  - Local Authority
  - NHS.

4. Objectives

- To ensure employees have a working knowledge into the principles and requirements of GDPR.
- To demonstrate that appropriate steps are taken to ensure The Superior Healthcare Group Ltd complies with GDPR when handling and using personal data provided by both employees and clients.
- To define accountability and establish ways of working in terms of the use, storage, retention and security of personal data.
- To assist with understanding and complying with our obligations in respect of the rights of the employees and clients who have provided personal data and the steps we will take if a GDPR breach occurs.

5. Policy

5.1. The General Data Protection Regulations (GDPR)

- The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way the Superior Healthcare Group carries out its data processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data.

- Superior Healthcare Group Ltd is a Data Controller or a Data Processor. We recognise that in most scenarios, we will be deemed to be a Data Controller (see Point 5.2).
- Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data.
- It is Superior Healthcare Group's policy to ensure that our compliance with the GDPR and other relevant data protection legislation is clear and demonstrable at all times.
- The vast majority of the personal data we process is on the legal basis that we must do so in order to execute contracts, or that we have a legitimate business interest to process it to run the business effectively.
- Some data, such as photographs or contact details for marketing, we use on the basis that we have consent from this individual to do so.

5.2. Data Protection Officer

- A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.
- Based on these criteria, the Superior Healthcare Group does not require a Data Protection Officer to be appointed. However, we have chosen to do so voluntarily. Our Data Protection Officer is Mark Povey, Director of JS Information Governance Ltd and can be contacted by telephone, email or post at:

  DPO
  Superior Healthcare Group Ltd
  Gazette House
  5 8 Estuary View Business Park
  Boorman Way
  Whitstable
  Kent
  CT5 3SE

  Email: dpo@superiorhealthcare.co.uk
  Tel: 01227 771133

- The Privacy Officer will be able to:
  - Be the main point of contact for any Subject Access Requests.
  - Be able to advise on correct storage and processing of data in line with current regulations (GDPR).
  - Advise the Company on any further changes or work needed in order to comply.
  - Assist to maintain the People Planner system in regards to the maintenance of data storage.
  - Assist with any other queries on data protection.

5.3. Definitions

- There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all as part of this policy. However, the most fundamental definitions with respect to this policy are as follows:

- **Data Protection Act 2018**: the Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive.
- **GDPR**: General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It was adopted on 14 April 2016 and after a two-year transition period became enforceable on 25 May 2018.
- **Data Subject**: the individual about whom The Superior Healthcare Group Ltd has collected personal data.
- **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, 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**: has 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.

5.4. Key Principles Relating to Processing of Personal Data

- The GDPR sets out the principles which we, as a data controller, must adhere to when processing personal data. The GDPR principles are as follows:
  - Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
  - Purpose limitation – data must be collected only for specified, explicit and legitimate purposes.
  - Data minimisation – data must be adequate, relevant and limited to what is necessary.
  - Accuracy – data must be accurate and, where necessary, kept up to date. Inaccurate data must be erased.
  - Storage limitation – data must only be stored for as long as is necessary.
  - Integrity and confidentiality – data must be processed in a secure manner.
- The Superior Healthcare Group recognises that in addition to complying with the key principles, we must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of a project, or engagement with a new client. Data protection should not be an after-thought.

5.5. Rights of the Individual

- The Data Subject has a number of rights under the GDPR. These are:
  - The right to be informed
  - The right of access

- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

- Each of these rights are supported by appropriate procedure that allows the required action to be taken within the timescales stated in the GDPR:

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access ('data subject access request')	One month
The right to rectification	One month
The right to erasure ('the right to be forgotten')	Without undue delay and no later than 1 month
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not specified

Table 1 - Timescales for data subject requests

5.6. Lawfulness of Processing

- The position has been improved under GDPR in terms of the ability of care sector organisations to process special categories of data. The provision of health or social care or treatment or the management of health or social care systems and services is now expressly referred to as a reason for which an organisation is entitled to process special categories of data.

- In terms of other types of personal data, The Superior Healthcare Group Ltd only processes personal data if it is able to rely on one of a number of grounds set out in GDPR. The grounds which are most commonly relied on are:

  - The Data Subject has given his or her **consent** to the organisation using and processing their personal data.
  - The organisation is required to process the personal data to **perform a contract.**
  - The processing is carried out in the **legitimate interests** of the organisation processing the data.
  - The processing is necessary to comply with a legal obligation.
  - The processing is necessary to protect the vital interests of the Data Subject or another living person.
  - The processing is necessary to perform a task carried out in the public interest.

6. Procedure

6.1. Initial Audits

- We conduct regular audits of the personal data we process. This is carried out internally with the assistance of key employees (usually our Compliance Team within the wider HR Department for the employees, and individual Nurse Managers auditing data collected at our clients' homes). We also undertake annual audit of our Data Protection processes via the NHS Data Security and Protection Toolkit, and the audits are completed in June every year. The audits reveal whether the ways in which we process personal data meet the requirements of Data Protection legislation.

6.2. The Right to be Informed

6.2.1. Fair Processing Notice / Privacy Notice

- Organisations are required to provide Data Subjects with certain information about the ways in which their personal data is being processed. We have determined that the simplest and most effective way to provide the required information is by issuing fair processing notices.
- The processing of personal data we carry out in respect of our employees will differ from the processing of personal data we carry out in respect of our clients or external parties. We will, therefore, produce and circulate at least two fair processing notices (privacy notices), one to employees and another to clients.
- The fair processing notices cover the processing of personal data that has been obtained other than through the company website. Collection of personal data via the website will be governed by the Website Privacy Policy and Procedure.

6.2.2. Consent Form

- The Fair Processing Notice sits alongside a consent form which can be used to ensure that we obtain appropriate consent, particularly from clients, to the various ways in which we use the personal data. The Consent Form contains advice and additional steps to take if the client is a child or lacks capacity.
- Under Data Protection legislation consent has to be:
    - Explicit - consent requires a very clear and specific statement of consent
    - Separate from other terms and conditions
    - Specific and 'granular' so that The Superior Healthcare Group Ltd gets separate consent for separate things. Vague or blanket consent is not enough.
- Processing Personal Data about children:
    - We will take extra care when processing personal data about children. GDPR does not specify an age at which children are deemed to be able to consent to their personal data being processed under GDPR (except where online services are being provided to a child, in which case a child can provide their consent at the age of 13).
    - We will seek consent in line with any relevant provisions in the Data Protection legislation and shall ensure that the ways in which we obtain consent from a child are appropriate. For example, we will obtain consent using language that is appropriate and easily understood by the child, taking into account the child's age and ability and the type of personal data being processed.

- We will use the template forms if we determine that we are required to seek consent from Data Subjects, including clients, to process their personal data under GDPR. We will seek further advice if we are uncertain as to whether consent is necessary.
- We will ensure we use the appropriate form, bearing in mind whether the Data Subject has capacity or lacks capacity.
- We will ensure that where children's services are provided or activities are undertaken where children might be present or involved, that parental/guardian consent is obtained in advance. This would include situations such as social events where photographs might be taken.

6.3. Subject Access Requests Process

- One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Data Subjects may ask The Superior Healthcare Group in writing by any means for access to their Personal Data. Where we receive a Subject Access Request, we will deal with them in accordance with the below process.
- **Stage 1** – **Maintaining a log of Subject Access Requests**
    - We will maintain a log of all the Subject Access Requests we receive, setting out the dates on which the requests are received and the final response sent, together with any intermediary steps taken before sending a final response (for example, request for identification proof or further information in respect of the data). If we fail to respond to the request in accordance with GDPR timescales, this will also be noted together with an explanation of the failure and steps taken to avoid such failure in the future.
- **Stage 2** – **Acknowledge Subject Access Request**
    - We will acknowledge receipt of the Subject Access Request, although this is not strictly necessary.
- **Stage 3** – **Confirmation of Identity**
    - We will only respond to a Subject Access Request if we are confident of the identity of the applicant.
    - We understand that it must be reasonable in terms of what we ask for and that we shouldn't ask for a significant amount of extra information if the identity of the person making the request is obvious, which is more likely to be the case if we have an ongoing relationship with that person. If, for example, an existing employee or client makes the request, we acknowledge that it is likely we will be able to confirm their identity easily.
    - If, however, we receive a request from an individual we do not recognise or the individual's email address/postal address has changed since our last dealings with them, we will consider seeking further proof of identity such as a recent utility bill or copy of a driving licence or passport.
    - In this scenario, the one-month time period to respond will commence only once we have received the proof of identity. We will not delay in asking for further proof.
- **Stage 4 – Checking if other information is required to find the records requested**
    - We are entitled to ask for further information needed in order to comply with the Subject Access Request, although it should not delay responding to a Subject Access Request unless we requires more information to find the data in question.
    - The Superior Healthcare Group Ltd should not require the applicant to narrow the scope of the request (they are entitled to ask for all the information The Superior Healthcare Group Ltd holds), but The Superior Healthcare Group Ltd may ask them to provide some context around the information they are

seeking such as relevant dates or if they want a particular document or type of document (for example, letter, email, application form), which may help The Superior Healthcare Group Ltd locate the data.

- The Superior Healthcare Group Ltd will not delay in asking for further information and will be clear about what details it needs. Provided it does that, and it needs the additional information in order to be able to comply (rather than it being a tactic to delay timescales), the one-month time period will begin when The Superior Healthcare Group Ltd receives the information.

- **Stage 5** – **Gathering information**
  - Collating all relevant information will be the most time-consuming task. We will consider which departments may hold personal data and whether that personal data can be accessed centrally by one individual or team.
  - The fewer people who are involved in locating the data, the less impact it will have on our day to day business.
  - We will consider how to search for the data. For example, does the Data Subject use a nickname or alternative name which would also need to be searched?
- **Stage 6 – Considering whether an exemption applies**
  - The Data Protection bill entitles a Data Controller to restrict Subject Access Requests to the extent that the restriction is necessary and proportionate to:
    - Avoid obstructing an official or legal inquiry, investigation or procedure.
    - Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.
    - Protect public security.
    - Protect national security.
    - Protect the rights and freedoms of others.
  - These are relatively narrow in scope, but we will consider them when responding to a Subject Access Request. If in doubt as to whether an exemption applies, we will seek legal advice.
  - If a request is manifestly unfounded or excessive, we may charge a reasonable fee or refuse to act on the request, but we will have to demonstrate that the request is unfounded or excessive. We are entitled to ask the Data Subject to specify the information or processing activities to which the request relates to.
- **Stage 7 – Maintaining confidentiality**
  - If personal data relating to other individuals is included in the documents that will be provided pursuant to the Subject Access Request, it will need to be redacted. We may alternatively obtain consent from the Data Subject to disclose the personal data, but that could be more time consuming than redaction.
- **Stage 8 – Reviewing what data has been requested**
  - In some cases, the Data Subject may only request a copy of his or her personal data.
  - They are entitled, however, to also request the following information:
    - The purposes of and legal basis for the processing.
    - The categories of personal data that are processed.

- The recipients or categories of recipients to whom the personal data has been disclosed.
- The period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine the retention period.
- The existence of the Data Subject's rights to request:
  - Rectification of personal data; and
  - Erasure of personal data or the restriction of its processing.
- The existence of the Data Subject's right to lodge a complaint with the Information Commissioner's Office and the contact details of the Information Commissioner's Office; and
- Communication of the personal data undergoing processing and any information about its origin.

- If the above information is requested in the Subject Access Request, it must be provided.

- **Stage 9 – Retention of information**
  - We will consider keeping a copy of the information provided to the Data Subject until we receive confirmation from the Data Subject that they do not require any further information, or for a period of **6 months** from completion of the request, whichever happens first.

6.4. Right to Erasure (Right to be Forgotten)

- employees have the right in certain circumstances to request to erase personal data that we hold about them. This is known as the right to be forgotten. Depending on the reasons and legal bases for processing the data, we may be required to erase some categories while we may have grounds for retaining others.
- If an employee or former employee asks us to delete data relating to them, we will identify our legal bases for processing the data and we will refer to the results from our data audit.
- We will not be required to erase data if they have a legal obligation to retain it. For example, employers have a duty to retain records relating to payment of statutory sick pay and statutory maternity pay for at least three years following the end of the tax year in which the payment was made.
- Where the legal basis for processing the data is the legitimate interests, we must delete the information if requested by the employee or former employee, unless there are compelling legitimate grounds for the processing that override the employee's interests, or the data is necessary for the defence of legal claims. For example, if an employee requests that the employer delete data relating to disciplinary proceedings against them, we could refuse the request on the ground that the data would be required should the employee bring a tribunal claim relating to the disciplinary issue.

6.5. Breach Notification Process

- We understand that if we breach GDPR, we may be required to notify the ICO as well as the Data Subjects who have been affected by the breach. We recognise that failure to report a breach could result in significant fines being imposed on The Superior Healthcare Group, as well as reputational damage.
- We recognise that we rely on our employees notifying our Data Protection Officer if they breach or think they may have breached GDPR. We will therefore encourage all of our employees to review the policy and understand their obligations in terms of **reporting a breach to the Data Protection Officer**.

- **What is a Breach?**
    - A breach of GDPR is any breach of security that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
    - Examples of a breach may include:
        - Sending an email to the incorrect recipient.
        - Copying rather than blind copying recipients of an email.
        - Losing a USB device containing personal data.
        - Leaving a hard copy of personal data (for example, a client record or employee file) in an easily accessible area so that details can be viewed or recorded, or the document taken.
        - Leaving a laptop or documents containing personal data on a train or other public transport.
        - Leaving a cupboard or filing drawer unlocked that contains personal data.
        - The above list is by way of example only and is not exhaustive or definitive.
- We will ensure that our employees understand that if they breach or think they may have breached GDPR, they should immediately notify our Data Protection Officer, who will determine the next steps to take.
- Once employees are aware of a breach of GDPR, the DPO deems to be aware of the breach, at which point the **72-hour timescale for notifying the ICO** will begin.

6.6. Criminal Offence Data

- The CQC requires that we, as CQC-regulated service provider, carry out DBS checks where we are authorised to do so under legislation. Certain roles will require either a standard, enhanced or enhanced with barred list information DBS check to be carried out.
- For those providing healthcare services, standard checks may be obtained for individuals working in a role listed in schedule 1 to the ROA (Exceptions) Order 1975 ("ROA Exceptions Order"). Paragraph 15 states: "Any employment or other work which is concerned with the provision of health services and which is of such a kind as to enable the holder of that employment or the person engaged in that work to have access to persons in receipt of such services in the course of his normal duties".
- An enhanced check may be obtained for the roles listed in the ROA Exceptions Order and also in the Police Act 1997 (Criminal Records) Regulations. Enhanced DBS checks with barred list information can be obtained for individuals where roles fall under the definitions of regulated activity within the meaning of the Safeguarding Vulnerable Groups Act 2006 as amended by the Protection of Freedoms Act 2012.
- We will only require a DBS check to be made where the role is eligible and the check shall be at the appropriate level only and no higher.
- We will assess the relevance of any cautions and convictions detailed in the DBS check to the role for which the applicant has applied.
- Given the sensitive nature of the information contained in a DBS certificate, we will ordinarily only retain on file information about the level of check which was requested, the number of the disclosure certificate and the date on which the certificate was obtained.

6.7. Data Storage

- As a general principle, we will not keep (or otherwise process) any personal data for longer than is necessary. If we no longer require the personal data once we have finished using it for the purposes for which it was obtained, we will delete the personal data.

6.7.1. Database Systems

- We use database systems to store a high proportion of our data. We use People Planner System and Sage Payroll system, for storing electronic employees records, and Income processing for clients' records and billing. Using these databases means that the majority of our data is in a structured, well ordered system, and access reporting and deletion are simple and effective.
- These products have also been, and will continue to be, updated to comply with the current GDPR.
- Access to all of these systems is carefully password protected and only key employees in the business can access them. The systems themselves are stored in a hosted environment which is protected by the database providers' security processes.
- To assist with GDPR compliance, we also use People Planner's own GDPR product/ programme. This product assists with the processing of Subject Access Requests and requests for personal data to be erased. This product is maintained and used by the authorised HR and Payroll team.

6.7.2. Storage of documents on the network drives

- Work produced digitally that may contain personal data should be stored on one of the company's shared drives or on 'Microsoft Teams'. This ensures all data is stored in a secure location and in an orderly manner, and that personal data can be easier located within the files if we need to locate it, correct it, or remove it.
- The 'Zone'
    - The Zone shared drive contains a set of folders that give space for different departments at our head office to store files. Instead of sending a file by email, the user can save it on the shared drive, and another user can obtain it from there.
    - In order for any personal data to be checked and removed if required, the Privacy Officer will also have access to these drives.
- The 'Microsoft Teams'
    - In a similar setup to the Zone, Teams is a shared connected network held on the central server, which our Head Office teams have access to.

6.7.3. USB sticks and personal laptops

- In order to maintain controlled storage and access to all data, including PID, it is essential that only company electronic devices are used. For example, no one employed by the Superior Healthcare Group is to bring and use their own personal laptop to work.
- The internal shared drives and Teams are set up, and user logins are protecting access to data. We have established processes for sharing and distributing data. USB sticks are a risk as data stored on them could easily be lost or copied. Most machines will therefore have their USB and SD card ports locked. Only the authorised senior management team's machines have a working USB and SD card port, for essential occasional use or for uploading information from external devices, such as cameras.

- No Employee should use a USB drive other than the Administration Team. The Teams and Zone drives are the correct way of sharing files between users.

6.7.4. Emails and attachments containing personal data

- Any sharing of PID is carefully controlled.
- Sending emails and information outside of the organisation:
    - Emails sent outside of the organisation must not contain PID in the title or body of the text. The information must be sent as a password protected attachment. For example, do not send an email to the CCG with a list of clients in our care and their dates of birth. Send an attachment, password protected, with the password on a separate email.
    - When sending information to multiple individuals, especially relatives for information or marketing purposes, ensure all email addresses are in the bcc box. This means no individual recipient will be able to see anyone else's email address.
    - When sharing confidential information with third party provider, use of password protected 'Teams' programme is advisable.
- Sending emails and information within the organisation:
    - Emails sent within the organisation should not contain PID in the title of the text. Only send PID information over email if essential to do so.
    - In preference to the above, use any of the secure shared network drives or Teams to store or share files for access by the recipient. This avoids sending the information through MS Outlook.

6.7.5. Windows User Logins

- For Each computer user has access to files based on their Windows login profile. Our IT team have set the passwords to require refresh every 60 days in order to help maintain security.
- If users leave the business or change roles, the IT company must be informed so that they can update the user Logins correctly.

6.8. Data Retention

- As a general principle, we will not keep (or otherwise process) any personal data for longer than is necessary. If we no longer require the personal data once we have finished using it for the purposes for which it was obtained, we will delete the personal data.
- When deciding how long we are required to keep records, we considered the data retention guidelines provided by the NHS. These are in line with the Records Management Code of Practice for Health and Social Care 2016 as per the below link. For more details regarding the retention periods please refer to our Retention Policy and Procedure.
    - https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice/
- For most of the personal data we process, we have a legal obligation to keep it for a number of years after the service termination with a client or employee contract. However, this must be kept in a well-ordered system as the data subject still has a right to ask to see the data we hold about them.

- For data relating to employee contracts, including pay and performance, we keep this for **7 years** after termination of the contract.
- For data relating to client contracts, including healthcare information, we keep this for **20 years** after termination of the contract, in line with the NHS Records Management Processes (as per the above).
- For data relating to recruitment or client enquiries, which are unsuccessful and therefore do not become part of our main employee or client databases, the retention period is **12 months** for employment candidates, and **18 months** for unsuccessful enquiries/referrals.
- A key principle of GDPR is that data held must be time-bound, meaning we should not keep personal data any longer than we need to.
- The archive stored at our Head Office in Whitstable (Gazette House) are cleared regularly so that any records pertaining to employees or clients exceeding the retention periods are marked for disposal. Once identified, these records can be disposed of, using a secure disposal service. We use external record storage company (Restore), which stores all the data in a secure data retention storage. Each stored box is labelled with a bar code corresponding to the description of the content and identified data retention period. Once we identify storage boxes and data to be deleted and destroyed, the request is sent to Restore and we receive confirmation certificated of the safe deletion of the data.
- Any data kept on any of our internal shared drives relating to the individual in question is also removed at that point by our internal IT Team.
- Emails must be cleared regularly so that non-essential emails older than 1 year are deleted.

6.9. Transfer of Data

- If we decide to transfer personal data to a third party, we will put in place an agreement to set out how the third party will use the personal data. The transfer would include, for example, using a data centre in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place.

6.10. Privacy Impact Assessments

- In addition to carrying out an Initial Impact Assessment, we will carry out further assessments each time we process personal data in a way that presents a “high risk” for the Data Subject. Given the volume of special categories of data that are frequently processed by organisations in the health and care sector, there are likely to be a number of scenarios which require a Privacy Impact Assessment to be completed.
- The Privacy Impact Assessment template may also be used to record any data protection incidents, such as breaches or 'near misses'.

6.11. Compliance with the GDPR

- We nominated an external Data Protection company **JS Information Governance Ltd** to act as our Data Protection Officer, responsible for data protection and GDPR compliance.
- We ensure that all employees understand the policies and procedures provided, including how to deal with a Subject Access Request and what to do if a member of our team breaches Data Protection regulations.
- We require all employees to take an online eLearning Data Protection training course and pass the assessment at the end.

- We conduct regular audits of the personal data currently held by The Superior Healthcare Group.
- We delete any personal data that we no longer need, in line with our Retention Policy, and taking into account any relevant guidance, such as the Records Management Code of Practice for Health and Social Care 2016.
- We will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with the Data Protection legislation.
- We regularly update and circulate Privacy Notice to clients and employees.
- We will ensure proper consent is obtained from each client in line with Data Protection regulations.
- We nsure that processes and procedures are in place to respond to requests made by Data Subjects (including Subject Access Requests) and to deal appropriately with any breaches or potential data breaches.
- We maintain a log of decisions taken and incidents that occur in respect of the personal data processed.

6.12. More information, complaints and updates

6.12.1. Access to personal information

- This policy and our fair processing notices may not provide exhaustive detail of all aspects of our collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to our Data Protection Officer:

  Data Protection Officer
  Superior Healthcare Group Ltd
  Gazette House
  5 8 Estuary View Business Park
  Boorman Way
  Whitstable
  Kent
  CT5 3SE

  Email: dpo@superiorhealthcare.co.uk
  Tel: 01227 771133

6.12.2. Complaints

- We will always try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.
- If you have a complaint about our use of your information, we would prefer you to contact us directly in the first instance so that we can address your complaint. However, you can also contact the Information Commissioner's Office via their website at www.ico.org.uk/concerns or write to them at:

  Information Commissioner's Office
  Wycliffe House
  Water Lane
  Wilmslow
  Cheshire

SK9 5AF

6.12.3. Updates

- We regularly review and, if appropriate, update this privacy policy from time to time, and as our services and use of personal data evolves. If we want to make use of personal data in a way that we haven't previously identified, we will contact the data subject to provide information about this and, if necessary, to ask for consent.
- We will update the version number and date of this document each time it is changed.