Policy No:
GIG 02.00

Policy and Procedure on

Data Protection

Policy Author / Reviewer	Russell Edge
Approval Date	September 2024
Next Review Date	September 2026
Version No	6
Policy Level	Group
Staff Groups Affected	All Staff

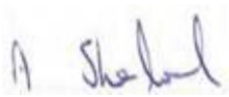
Contents

1. Monitoring and Review

1.1. The Proprietor will undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than two years from the date of approval shown above, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

1.2 This policy will also be reviewed earlier if new data protection legislation such as the Data Protection and Digital Information (DPDI) Bill (when enacted) introduces requirements that affect the Company's processing activities

Signed:



Amanda Sherlock
Senior Information Risk Owner (SIRO)
Director, Compliance & Regulation
September 2024

2. Terminology

2.1. Our aim is to use consistent terminology throughout this policy and all supporting documentation as follows:

Personal Information/ Personal Data	Personal information is any information about any living person from which they can be identified. This can be on paper, on a computer or even just talked about. Personal information can relate to, for example, past or present employees/workers, contractor/suppliers, patients, service users, residents, customers or shareholders. Some examples are: personal contact details, such as name, address, email, telephone number, date of birth, bank account details.
Special Category of personal information/Sensitive Personal Information	Information about an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; criminal convictions, offences or alleged offences; genetic data; or biometric data for the purpose of uniquely identifying an individual.
Processing	Any activity that involves using personal information. This includes collecting personal information, recording it, storing it, retrieving it, using it, amending it, disclosing it, destroying it, and transferring it to third parties.
Data Protection Impact Assessment	An assessment required when processing is likely to result in a high risk to individuals. This includes traditional Data Protection Impact Assessments and any assessment of high-risk processing as described in the latest ICO guidance
Artificial Intelligence (AI) Processing	The use of automated systems, including machine-learning tools, that analyse personal data to identify patterns, make predictions, or support decision-making.
Direct Marketing	Direct marketing means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.
'Establishment' or 'Location'	This is a generic term which means the Children's/Patient's/Service Users Home/school/college
Individual/Data Subject	This means the person whose personal information is held by the Company.
Service Head / Head of Service	This is the senior person with overall responsibility for the Location. For Cambian Dilston College this is Marie Flatman (Principal), and Rick Johnson who is Registered Manager/Head of Care.
Regulatory Authority	Regulatory Authority is the generic term used in this policy to describe the independent regulatory body responsible for inspecting and regulating services.

Social Worker	This means the worker allocated to the child/family. If there is no allocated worker, the Duty Social Worker or Team Manager is responsible.
Placing Authority	Placing Authority means the local authority/agency responsible for placing the child or commissioning the service.
Staff	Means full or part-time employees of the Company, agency workers, bank workers, contract workers and volunteers.

3. Introduction

3.1. The Company is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees under the Data Protection Act 2018 and the General Data Protection Regulations (UK GDPR). The Company will ensure this policy is updated in line with changes to UK data protection law, including forthcoming reforms under the Data Protection and Digital Information (DPDI) Bill."

3.2. This policy sets out how the Company deals with personal data and applies to CareTech and all of its direct and indirect subsidiaries and references to "the Company" shall be construed as referring to all such companies.

3.3. It affects all staff and must be read in conjunction with the following policies:

- Information Security (GIG 04)
- Risk Management (GIG 05)
- Records Management (GIG 06)
- Information Systems Acceptable Use (GIG 07)
- Access to Records (GIG 08)
- Confidentiality Code of Practice (GIG 09)
- Processing of Special Category Data and Criminal Offence Data (GIG 02.07)
- Remote Working Policy

3.4 The Company shall maintain, as required, certain personal data about living individuals for the purposes of satisfying operational requirements and legal obligations.

3.5 The need to process data for the Company's operational purposes should be communicated to all data subjects. Further information of the Company's operational purposes and how it handles personal data is outlined in the Privacy Policy which is available on the website.

3.6. The types of personal data that the Company may hold includes information about:

- current, past and prospective employees;
- current, past and prospective students and residents;
- individual staff members of placing authorities;
- individual staff members of suppliers;
- Shareholders, foster parents and others with whom it communicates.

3.7. Personal data, whether it is held on paper, on computer or other media, shall be subject to the appropriate legal safeguards as specified in the General Data Protection Regulations 2016 (UK GDPR) and Data Protection Act 2018.

3.8. The Company have appointed a Data Protection Officer who is ultimately responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Information Governance Board. Any questions or concerns about the interpretation or operation of this policy should be taken up, in the first instance, with the Data Protection Officer who can be contacted at: Data.Protection@CareTech-UK.Com.

4. Purpose

4.1. The purpose of the Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the UK GDPR and Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default. All processing activities must follow the principles of data protection by design and by default, ensuring privacy is embedded into systems, decisions, and processes

5. Scope and Consequences for Non-compliance

5.1. All Employees, irrespective of their role within the organisation, are held by the contents of this policy and are required to follow and uphold the values, principals and expected behaviours of the Company when carrying out their duties and responsibilities.

5.2. With regards to data protection, the roles and responsibilities of employees are set out at the end of this policy (see Appendix 1).

5.3. All Employees and others who obtain, handle, process, transport and store personal data for the Company are under an obligation to ensure that they have regard to the six data protection principles (see below) when accessing, using or disposing of personal information.

5.4 Failure to observe the data protection principles within this policy may result in an Employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an Employee accesses another Employee's employment records without the requisite authority, the Company will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

6. Principles

6.1. The Company fully endorses and adheres to the six principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. The Company will retain its data and records in accordance with the requirements of ISO 9001/2015 and other appropriate Regulations and Standards.

The Data Protection Principles

6.2. The principles require that personal information must be:

a) Processed lawfully, fairly and in a transparent manner;
b) Collected only for specified, explicit and legitimate purposes, and processed only in line with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) Accurate and, where necessary, kept up to date;
e) Not kept in a form which permits identification of individuals for longer than necessary, in relation to the purposes for which it is processed;
f) Kept secure, and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Satisfaction of principles

6.3. In order to meet the requirements of the principles, the Company shall:

a) make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

b) ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

c) not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

d) review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the Company if, for example, a change in circumstances mean that the data needs to be updated. It is then the responsibility of the Company to ensure that any notification regarding the change is noted and acted on.

e) undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the Company will undertake a regular review of the information held and implement a weeding process. The Company will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

f) only process personal data in accordance with individuals' rights (these rights are listed below). All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. The Company will ensure that all personal data is accessible only to those who have a valid reason for using it.

g) have in place appropriate technical and organisational security measures to safeguard personal information; ensure that personal information is not transferred to countries outside of the United Kingdom without notifying the Data Protection Officer and that suitable safeguards are in place.

h) Ensure that where automated or AI-assisted processing is used, meaningful human oversight is maintained and individuals are informed where required.

7. Notifying the Data Protection Officer of certain activities

7.1. A Data Protection Impact Assessment must be undertaken prior to undertaking certain activities that involve processing personal information.

7.2. A 'data protection impact assessment' will consider the impact of the activities on individuals; identify privacy risks and steps to minimise those risks; and evaluate whether the activities are permitted by data protection law.

7.3 Employees should seek advice from the Data Protection Officer so they can advise whether a data protection impact assessment is required in the following situations:

a) Process new types of personal information i.e. personal information which has not been collected before.
b) Process personal information in a new or significantly different way, including via the use of new technologies.
c) Use personal information for a purpose other than that for which it was collected.
d) Enter a contract with a third party that involves disclosing or sharing personal information.
e) Any new or significantly different use of automated processing of personal information to evaluate an individual, for example to analyse or predict an individual's performance at work, health, personal preferences, interests, reliability, behaviour, location or movements.
f) Any new or significantly different use of automated decision-making i.e. where a decision is made on a solely automated basis without meaningful human involvement, and it has a significant effect on individuals.
g) Any new or significantly different large-scale processing of special categories of personal information; or large scale, systematic monitoring of a publicly accessible area. Whether processing is 'large scale' will depend on, for example, the number of individuals, volume of data, range of data, duration of processing, or geographical extent – if you are in any doubt as to whether processing is large scale, contact the Data Protection Officer.
h) Implement significant changes to systems or the business (including new or different technology) which involve processing personal information.
i) Any direct marketing activity to individuals (including electronic marketing by email, telephone, fax or text message).
j) Transmit or send personal information to, or view or access personal information in, a country outside of the United Kingdom where this has not been previously authorised by the Data Protection Officer or in line with the Group's Data Protection Policy.
k) Any processing that involves Artificial Intelligence (AI) tools or automated analytics that could influence decisions about an individual.

7.4. Employees must comply with any directions from the Data Protection Officer in relation to the above, and the terms of any data protection impact assessment.

8. The lawful bases for processing personal information

Non-Sensitive Personal Data

8.1. The Company will only process personal data where it is strictly necessary to carry out a specific purpose. The processing of personal data must be based on one of the legal bases listed below:

a) the data subject has given his or her consent.
b) the processing is necessary for the performance of a contract with the data subject (e.g. monitoring performance of employees in line with the contract of employment) or where the data subject has requested the Company to take specific steps before entering into a contract (e.g. obtaining employment references from a previous employer).
c) to meet our legal compliance obligations (safeguarding children, for example).
d) to protect the data subject's vital interests (i.e. matters of life or death).
e) to perform a task in the public interest or for our official functions where the task or function has a clear basis in law.

f) to pursue the Company's legitimate business interests providing there is no conflict with the data subjects rights. Where legitimate interests are relied upon, a Legitimate Interests Assessment (LIA) must be completed and documented.

Sensitive Personal Data

8.2. The processing of sensitive personal data represents a greater intrusion in individual privacy than when processing non-sensitive personal data. We will therefore take special care when processing sensitive personal data, in particular in ensuring the necessity of the processing and security of the information.

8.3 The processing of sensitive personal data must be based on one of the above legal bases for processing non-sensitive personal data **and** one of the additional legal bases below for processing sensitive personal data:

a) The data subject has given explicit consent.
b) The processing is necessary in the context of employment law, or laws relating to social security and social protection.
c) The processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving consent.
d) The processing relates to personal data which have been made public by the data subject.
e) The processing is necessary for the establishment, exercise or defence of legal claims.
f) The processing is necessary for reasons of substantial public interest**,** and occurs on the basis of a law, it is proportionate to the aim pursued and protects the rights of data subjects.
g) The processing is required for the purpose of medical treatment undertaken by health professionals**,** including assessing the working capacity of employees and the management of health or social care systems and services**.**
h) The processing is necessary for reasons of public interest in the area of public health.

8.4 Sensitive personal data must be processed in keeping with the **Policy for Processing Special Categories of Personal Data and Criminal Offence Data**.

9 . Criminal Convictions Data

9.1. There are specific rules regarding the processing of data relating to criminal convictions and offences. Such data must be processed in keeping with the **Policy for Processing Special Categories of Personal Data and Criminal Offence Data**. Advice should be sought from the Data Protection Officer as required.

10. Consent

10.1 Consent is:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

10.2. Consent means giving people genuine choice and control over how we use their data. If the individual has no real choice, consent is not freely given and it will be invalid. This means people must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time. It also means consent should be separated from other terms and conditions (including giving separate consent options for different types of processing) wherever possible.

10.3 Whilst consent is one of the legal bases for processing of personal information, it is not required where another legal basis exists. Where consent is required, the data subject must be informed and their wishes must be respected and written record must be retained for auditing purposes.

10.4 The Company will only obtain an individual's consent where there is genuine choice and genuine control by the individual whether or not to consent to the processing of their personal information. We will rely on other legal bases where they are appropriate for the processing. Where consent is used as the lawful basis, the Company will ensure that consent is refreshed at appropriate intervals and remains valid, informed, and up to date.

10.5. Personal data or photographs will not be used in newsletters, websites or other media without the consent of the data subject. We will seek consent before displaying within our Locations, personal information about individuals (including, certificates/qualifications). Routine consents will be incorporated into the Location's individual's care data gathering sheets to avoid the need for frequent, similar requests for consent being made by the Location.

10.6. Consent will not be required to publish information already in the public domain. This would include, for example, information on staff contained within externally circulated publications such as Bulletins and Locations' Parent Newsletters. Any employee who wishes to withdraw their consent to their data being circulated in such publications should contact the Human Resource Director.

10.7 Where the individual lacks the capacity to consent, a 'best interest' assessment must be undertaken to inform the decision-making process.

11 . Children

11.1. Communications aimed towards children and young people must be clear and concise. It should be age-appropriate and presented in a way that appeals to a young audience.

11.2. Where we rely on consent as the lawful basis for processing information about children and young people, we will obtain consent from children aged 13 and over **where the processing relates to information society services**. For other contexts such as education, care, or safeguarding settings, consent will be sought from the person with parental responsibility unless the young person is deemed competent to decide.

11.3. Where parents have separated or the young person lacks the capacity to consent, consideration should be given to the 'best interests' of the child/young person.

12. Direct Marketing

12.1. Direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

12.2. The Company will not participate in direct marketing practices in the absence of:

- Explicit consent from the data subject
- A legitimate business interest reason (in this case, advice must be sought from the Data Protection Officer)

12.3. Even where legitimate interests or explicit consent has been established, all correspondence and the relevant webpages/emails must include opt-out options.

12.4. All individuals must be given the opportunity to opt-in to receive material at the point of data collection. The appropriate opt-in mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

13. Data security and Retention

13.1. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted. All systems must use multi-factor authentication (MFA) where available, and devices used to access personal data must be encrypted in line with current cyber-security best practice

13.2. All staff are responsible for ensuring that:

- any personal data which they have access to is kept securely;
- personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party;
- computer workstations in administrative areas are positioned so that they are not visible to casual observers and are not left unattended when the user is still logged-on or in any other circumstances when the personal details of staff or individuals in our care could be accessed by unauthorised persons;
- papers containing personal information are stored where they are not accessible to anyone who does not have legitimate reason to view or process them and they are not left on view in circumstances in which they could be read by unauthorised persons;
- particular care and measures are taken to protect sensitive personal information from unauthorised access.
- Staff must immediately complete any cyber-awareness or phishing-prevention training provided by the organization.

13.3. The Head of Location/Team Manager is ultimately responsible for ensuring that data is restricted internally to only those individuals or groups of persons who need access to any data through the course of their work role.

13.4. The Company needs to retain information whilst service users and employees remain looked after or employed by it and for a period after the relationship terminates in accordance with statutory limitation periods and the Company's Data Retention Schedule. All staff are responsible for ensuring that information is not kept for longer than necessary.

14. Right to Access Information

14.1. Employees and other subjects of personal data held by the Company have the right to access any personal data that is being kept about them electronically and also have access to paper-based data held in certain manual filing systems.

14.2. All individuals who are the subject of personal data held by the Company are also (in some circumstances) entitled to:

a) The right to be informed about the information we collect about them and how we handle it
b) The right of access to their personal information
c) The right to rectification of their personal information
d) The right to erasure of their personal information
e) The right to restrict processing of their personal information
f) The right to transfer their personal information to another person or organisation
g) The right to object to processing of their personal information
h) The right not to be the subject of any automated decision-making by us using their personal information or profiling them
i) The right to lodge a complaint with the Information Commissioner's Office (ICO).

14.3 These rights are subject to certain exemptions which are set out in the General Data Protection Regulations (UK GDPR) and Data Protection Act 2018. Therefore, requests from individuals regarding their personal information must be handled in line with the **Access to Records policy (GIG 08)**; and advice must be sought from the Data Protection Officer. We will verify the identity of any person making a rights request to ensure information is not disclosed unlawfully.

14.4. All enquiries about the handling of personal information must be dealt with promptly and courteously.

15. Data Disclosures

15.1. Personal data will only be disclosed to organisations or individuals for whom the data subject's consent has been given, or organisations that have a legal right to receive the data without consent being given.

15.2. When requests to disclose personal data are received by telephone it is the responsibility of the Company to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

15.3. If a request is made in person for personal data to be disclosed it is the responsibility of the Company to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

15.4. Personal data should only be disclosed to Police Officers if they are able to supply formal, specific written confirmation of a specific, legitimate need to have access to specific personal data e.g. to assist in criminal investigations.

15.5. A record should be kept of any personal data disclosed as an audit trail and so that the recipient can be informed if the data is later found to be inaccurate.

16 Passing Information to Partners, Relatives or Carers

16.1 When clients are admitted to any Service/hospital/facility they must be asked for consent to pass on information about their condition and progress, including to partners, relatives or carers. If consent is refused this must be recorded in such a way as to ensure all staff answering enquiries are made aware of the client's wishes.

16.2. If a client is unable to give consent (e.g. unconscious or otherwise unable to understand what is required), information about his/her condition must only be given to the person who is judged to be the next of kin. This would usually be the spouse or partner. In the case of a widow or widower or someone without a partner, the parent and any children of that client have an equal right to information. If none of these relationships exist, a brother or sister would have a right to information. Outside of this, advice should be sought from the Multi-Disciplinary Team before passing on information to other relatives. Staff must be particularly sensitive when passing information about clients with a learning disability. Itmay be appropriate to share information or discuss a client's care with someone who has a formal caring role for that individual. This must only be done where it is clearly seen to be in the best interest of the client. Information shared must be limited only to that which is required for the ongoing care of the client.

16.3. It is recommended good practice, in the case of clients unable to give consent that a record is made of the information provided and to whom it has been provided. If the client subsequently becomes fit to consent, he/she must be advised of the information that has been given and to whom it has been given, and must be asked for consent to continue to pass on information.

16.4. Clients under 16 are entitled to the same duty of confidence as adults and must be asked for consent to pass information to relatives, carers, etc. Young People under 16 who have the capacity and understanding to take decisions about their own treatment are entitled also to decide whether personal information may be passed on and generally to have their confidence respected. In these circumstances professional staff will be consulted.

16.5. Client information, including condition reports and future appointment dates, should not be given out over the telephone unless permission has been given by the patient or client, or there is no doubt as to the caller's entitlement to the information. As a general rule, only basic information should be provided although it may be appropriate to provide more detailed information to immediate family members entitled to information who live a distance away. In all cases, staff must be satisfied that the person has a right to the information and that the patient or client has not objected.

17 Photographic, Audio & Video Recordings and Use of Data on Social Media

17.1 In all cases, of photographic, audio and video recordings, consent is required and refusal to participate must be respected. Consent can be given verbally and recorded and dated in the client's notes. The completion of a consent form is recommended where recordings or images are likely to be published.

17.2 In all cases, the client must be informed, in a way he/she can understand, why the recording/images are being taken and how they will be used. Otherwise, consent will not be valid. The person responsible for seeking consent is the person requesting the image or recording.

17.3. Images taken as part of care and treatment are confidential. A hard copy must be placed in the client's record and must be protected in the same way as any other confidential document within a health or social care record. Once the hard copy is made, the image must be deleted from the camera/PC.

17.4 For reasons of privacy and confidentiality, service users, relatives and other visitors should also be discouraged from using personal phones or cameras to take photographs on Company premises.

17.5. Social media must never be used in a way that conflicts with or breaches any organisational policy. Personal confidentiality of employees or clients must be respected at all times.

17.6. Social media should not be used to make defamatory or disparaging comments about any employee, service user or any business partners of CareTech.

17.7 Employees should not post any material that identifies or could potentially identify the location of any children's care services.

17.8 Employees will be personally responsible and accountable for any images that breach confidentiality or contain sensitive information; are speculative or discriminatory or contain information that might identify a service user.

17.9 Staff must not create, upload, or share AI-generated or synthetic media (including deepfake images or videos) involving service users, staff, or Company locations

18 Removal of Patient/Client Records from Company Premises by Staff

18.1 The removal of client records from premises by staff, except in the following circumstances, is prohibited:

- When a client is being transferred for care or treatment to another service.
- When a member of staff is making a domiciliary visit and must take a client's notes along.
- When notes are needed for evidence in a court case and the attending member of staff cannot collect them on the day of the hearing.
- When a professional has a visit outside the client's residence or office premises and needs to take notes or requires them for updating following a consultation which may entail taking records home overnight.
- When other working practices require professional staff to take records home overnight (to be returned to premises the next working day).

19 Transferring Personal Information outside of the United Kingdom

19.1. There are strict guidelines regarding the sharing of information outside of the United Kingdom.

19.2. Before transferring personal data outside the UK, the Company must complete a Transfer Risk Assessment (TRA) and ensure an appropriate transfer mechanism is in place, such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses.

20 Personal Information Breach

20.1. A personal information breach is a breach of security leading to the accidental or unlawful destruction of personal information; loss, alteration, unauthorised disclosure, or access to personal information transmitted, stored or otherwise processed.

20.2. If you know or suspect that there has been a personal information breach, you must report it immediately to your line manager and the Data Protection Officer. You must also take action to stop the breach getting worse, for example, by:

a) Confirming that an email has been deleted by the recipient following accidental disclosure, or if possible, revoke any further access.
b) Recovering lost paper records or any lost device left in a public place.
c) Changing the access codes to any compromised building.
d) Informing IT in the event of any compromised computer or data access or anything suspicious or untoward on your device, applications or network files & folders.
e) Disconnecting your device from the network and report directly to IT, if you suspect you are being directly targeted in a cyber-attack.
f) Where a reportable breach occurs, the Company must notify the Information Commissioner's Office (ICO) within 72 hours in accordance with UK GDPR requirements

20.3 In order to reduce the potential for data breaches all staff are required to comply with the requirements of this policy and in particular Appendix 2, below.

21 Appendix 1: Roles and Responsibilities

21.1 The Board of CareTech Group

The board of CareTech Group is responsible for all governance within CareTech and its associated companies.

21.2 The Senior Management Team

The Senior Management Team has responsibility for information governance. This involves providing high level support to ensure that each service applies relevant information governance policies and controls, including compliance with the requirements of the Data Protection Act 2018/UK GDPR

21.3 The Data Protection Officer

The Data Protection Officer is responsible for:

a. Acting as the first point of contact for all data protection issues
b. Providing guidance and advice on data protection issues
c. Renewing and amending the Company's data protection notifications to the Information Commissioner
d. Coordinating the timeliness of responses to subject access requests and other requests from data subjects
e. Overseeing all data sharing protocols and agreements
f. Creating, maintaining and renewing training modules and toolkits as appropriate
g. Providing data protection training and awareness raising
h. Coordinating and investigating information breach procedures.
i. Ensure compliance with and review of the NHS Data Security and Protection Toolkit (DSPT) and all annual updates

The Data Protection Officer must operate independently and must not be instructed on how to perform their tasks. The DPO must not be dismissed or penalised for carrying out their statutory duties

21.4 Department/Line Managers

Department/Line Managers are responsible for ensuring that this policy and any associated procedures governing the use of personal information are understood and followed by all staff within their service. In addition, they must:

a. Ensure that their staff has access and resources to receive data protection training appropriate to their role
b. Report any suspected breaches of confidentiality or information loss to the Data Protection Officer and follow any subsequent procedures
c. Identify any existing or emerging information risks relating to personal information and report to the Data Protection Officer
d. Ensure the timeliness of responses to subject access requests and other requests from data subjects
e. Ensure that there are appropriate procedures and measures in place to protect personal data, particularly when that information (hardcopy and electronic) is removed from the Company's premises
f. Undertake annual information self-assessments to ensure on compliance with this policy
g. Consult the Senior Management Team and Data Protection Officer before entering into any information sharing protocol or agreement.

21.5 Employees

Employees have a responsibility for data protection and must:

a. Read, understand and follow this policy and any associated procedures that relate to the use and handling of personal information in the course of their work
b. Undertake data protection training and ensure they have a clear understanding of their responsibilities when handling personal information
c. Identify and promptly report any risks to personal information to their line manager and/or the Data Protection Officer
d. Identify and report suspected breaches of confidentiality or compromised personal data to their line manager and/or the Data Protection Officer
e. Identify and forward any subject access requests to the Data Protection Officer to ensure that requests can be processed in accordance with the statutory timescales
f. Assist clients in understanding their information rights and the Company's responsibilities in relation to data protection.
g. Ensure that any personal data that they provide to the Company is accurate and up to date and inform the Company of any changes to personal information which they have provided, e.g. changes of address.

22 Appendix 2: Handling Personal Information Securely

22.1 Emailing Personal Data

a. Before sending personal or confidential information by email, always double-check that recipient names, email addresses, and attachments are correct.

b. Do not forward unnecessary email trails and always double-check that the content is appropriate.

c. Limit the amount of personal data that you send to only that which is necessary.

d. When emailing more than one recipient, use the 'Bcc' function to hide recipients' identities, unless there is a legitimate reason why the names and email addresses of recipients would need to be shared.

e. When sending particularly sensitive information, consider asking a colleague to undertake the above checks for you (known as a "peer check")

22.2 Posting Personal Data

a. Before sending personal data by post, always double-check that you are sending the information to the correct recipient and that you have addressed the envelope fully and correctly.

b. Always check that any documents you are sending have not been mixed up with other

c. Clearly mark the envelope or parcel “private and confidential” and/or “to be opened by addressee only”, and include a return address. Use secure postage/delivery services appropriate to the sensitive nature of the information.

d. When sending particularly sensitive information, consider asking a colleague to undertake the above checks for you (known as a “peer check”)

22.3 Office Security

a. Lock your computer screen when you leave your desk.

b. Ensure that visitors are accompanied at all times whilst in the building.

c. Destroy or dispose of paper files securely

d. Do not print personal data unless absolutely necessary and do not leave the printer unattended whilst printing personal data.

e. Keep your desk clear of any papers besides those required at a particular time.

f. All personal or confidential information held in any form; e.g., paper, CD, memory stick, etc. must be locked away when unattended.

22.4 Carrying Personal Data Off-Site

a. Confidential documents/materials or documents containing personal information, must not be taken out of the office without specific authorisation from a line manager. Taking paper records/hard copy material off-site should only happen when it is absolutely essential to do so and there is no alternative method for accessing the information or undertaking the work. Records should not be taken off-site just because it is convenient to do so.

b. Where papers records/hard copy material have to be taken off-site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed and, where possible, data should be anonymised.

c. Carry paper files in a locked briefcase or in a folder or bag that can be securely closed or zipped up. Ensure that the briefcase/folder/bag contains your name and contact details.

d. Never leave paper files, laptops or mobile phones unattended, even for a short time. Lock them away or keep them with you.

e. Count how many files you have before you set off and check that you have the same number of files prior to leaving all destinations.

f. All devices used off-site must be encrypted and protected with multi-factor authentication

22.5 Social Media, Messaging Platforms and personal and work mobile devices

a. Personal devices (e.g. mobile phone or iPad) must not be used to capture or store any information in any format (text, picture, video, attachments) about service users, staff, customers or clients.

b. Any information about staff, service users, customers or clients must be captured or shared using a company- issued device. The information should then be transferred onto the company's information management systems and then deleted from the mobile device.

c. Personal Identifiable Information about staff, service users, customers or clients must not be shared or stored on WhatsApp or other messaging platforms.

d. Social media and personal blogs (such as Facebook, Twitter, LinkedIn or Instagram)
Employees should refrain from sharing confidential or sensitive information related to the organisation or individuals in our care unless it is a company account and all permissions have been checked and safely filed. The information includes – photographs, statements, personal histories and any personal identifiable information.

e. Personal data must not be stored on personal cloud storage services such as personal Google Drive, Dropbox, or iCloud accounts

23 Document Change Control

Date of Issue	Version No	Brief description of change
September 2023	V6.0	Approved Version – Updates to the following sections including Social Media, Dates and approval information.
September 2024	V7.0	Approved Version – Updates to sections including AI, and leglisation/regulations.