Grateley House School

Data Protection Policy
2025-26

Policy written by	Russell Edge, Senior Information Risk Owner (SIRO) & Data Protection Officer
Date of Review	September 25
Date of SLT review	January 26
Date of Next Review	September 2027

Introduction

CareTech 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) 2021.

Summary

This policy sets out how CareTech deals with personal data and applies to CareTech and all its direct and indirect subsidiaries and references to CareTech shall be construed as referring to all such companies. CareTech will keep certain personal information about individuals when needed to meet business needs and legal requirements. CareTech must inform individuals about why their data is being used for business operations. More details about these purposes and how personal data is managed can be found in CareTech's Privacy Policy, available on its website.

The types of personal data that CareTech may hold includes information about:

- Current, past and prospective employees
- Current, past and prospective students and people who use our services
- Individual staff members of placing authorities
- Individual staff members of suppliers
- Shareholders, foster parents and others with whom it communicates
- 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 2021 (UK GDPR) and Data Protection Act 2018.

CareTech has appointed a Data Protection Officer (DPO) who is responsible for making sure they follow the Data Protection Act and carries out this policy on behalf of the Information Governance Board. If you have any questions or concerns about how this policy is understood or applied, please contact the DPO first at Data.Protection@CareTech-uk.com

Purpose

This Data Protection Policy is designed to support key standards and laws, including the 7 Caldicott Principles, the 10 Data Security Standards, the UK GDPR, the Data Protection Act 2018, and the common law duty of confidentiality. We believe that protecting personal data is a fundamental right and are committed to applying data protection principles from the start and by default in everything we do.

Scope

Employee Responsibilities and Data Protection

- All employees, no matter their role, must follow this policy and uphold the CareTech values, principles, and expected behaviours in their work.
- Specific responsibilities related to data protection are listed in **Appendix 1.**
- Anyone who collects, uses, processes, moves, or stores personal data on behalf of CareTech must follow the **seven data protection principles** (see below) when handling personal information.
- Breaking these principles can lead to serious consequences. Employees may face **criminal charges** and **disciplinary action**, including dismissal. For example, if someone accesses another employee's records without proper permission, it will be treated as **gross misconduct** and could also be a **criminal offence**.

Reporting Concerns

If there's a concern about a data asset, it should be reported to both the **Information Asset Owner (IAO)** and the **Data Protection Officer (DPO)** so that it can be properly assessed.

Information Asset Owners (IAO)

IAOs are responsible for making sure their projects, initiatives, or data processing activities follow this policy and all relevant data protection laws.

They must:

- Provide assurance to the **Senior Information Risk Owner (SIRO)** that proper controls are in place.
- Carry out a **Data Protection Impact Assessment (DPIA)** for any new project, system, or process involving personal data.
- Make sure the **DPO** is involved in the DPIA process

Heads of Locations

School Heads and Registered Service Managers are responsible for:

- Ensuring compliance with data protection within their location.
- Promoting good data protection practices.
- Assessing any new or significantly changed personal data processing to determine if a DPIA is needed.
- Consulting the **DPO** promptly on any data protection issues.

Senior Information Risk Owner (SIRO)

The SIRO uses DPIAs to confirm that personal data is being processed securely and responsibly.

If a DPIA identifies major risks to the Group, the SIRO is responsible for reviewing and approving it.
Data Protection Officer (DPO). As required by **GDPR**, the Group has appointed a DPO to:

- Advise and guide the organisation on data protection responsibilities.
- Support and monitor DPIA processes.
- Communicate with the **Information Commissioner's Office (ICO)** when necessary.

Principles

CareTech fully endorses and adheres to the seven principles of the Data Protection Act. A guide to the data protection principles | ICO These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. CareTech will retain its data and records in accordance with its Policy and Procedure on Records Management appendix 3 Retention and Archive Periods.

Meeting Data Protection Principles

To comply with data protection principles, CareTech will:

Keep individuals informed: Make sure people know who is responsible for their data (the data controller), why their data is being used, who it might be shared with, how long it will be kept, and any other relevant details.

Use data only for its original purpose: Only use personal data for the reason it was collected—unless the individual is told about any new use before it happens.

Collect only necessary data: Avoid collecting personal data that isn't needed. Data collection forms will be designed with this in mind. Any extra or irrelevant data provided will be deleted immediately.

Keep data accurate and up to date: Individuals must inform CareTech if their personal details change. CareTech will then update its records accordingly.

Don't keep data longer than needed: Regularly review stored data and remove anything that's no longer necessary. Data will be securely deleted or destroyed to protect privacy (e.g., shredding paper files or securely deleting electronic records).

Respect individuals' rights: Only process personal data in line with people's rights. Staff must keep data secure and avoid sharing it with anyone who isn't authorised. Access to personal data will be limited to those with a valid reason.

Protect data with strong security: Use appropriate technical and organisational measures to keep data safe. Personal data won't be sent outside the UK without informing the Data Protection Officer and ensuring proper safeguards are in place.

Notifying the Data Protection Officer (DPO)

Before starting any activity that involves handling personal data, a **Data Protection Impact Assessment (DPIA)** must be completed. A DPIA helps:

- Understand how the activity might affect individuals
- Identify privacy risks and how to reduce them
- Check if the activity complies with data protection laws

Employees should speak to the **Data Protection Officer** to find out if a DPIA is needed in situations such as:

- Collecting new types of personal data not previously gathered
- Using personal data in a new or significantly different way, including with new technology
- Using personal data for a different purpose than originally intended
- Signing contracts with third parties that involve sharing personal data
- Using automated systems to evaluate individuals (e.g. predicting work performance, health, preferences, behaviour, location)
- Making decisions using automated systems without human input, especially if it significantly affects individuals
- Carrying out large-scale processing of sensitive personal data or monitoring public spaces—if unsure whether it's "large scale," ask the DPO
- Making major changes to systems or business processes that involve personal data
- Running direct marketing campaigns (e.g. emails, calls, texts)
- Sending or accessing personal data in countries outside the UK, unless already approved by the DPO or covered by the Group's Data Protection Policy

Employees must follow any instructions given by the **Data Protection Officer** and comply with the terms of any DPIA.

Lawful Bases for Processing Personal Information

Non-Sensitive Personal Data

CareTech will only process personal data when it's absolutely necessary for a specific purpose. This must be based on one of the following legal grounds:

- The individual has given their consent
- It's needed to carry out a contract with the individual (e.g., monitoring employee performance), or to take steps before entering into a contract (e.g., checking references)
- It's required to meet legal obligations (e.g., safeguarding children)
- It's necessary to protect someone's life or health (vital interests)
- It's needed to carry out a task in the public interest or an official duty backed by law
- it supports CareTech's legitimate business interests, as long as it doesn't override the individual's rights

Sensitive Personal Data

Sensitive data (like health, race, religion, etc.) requires extra care because it affects privacy more deeply. We must ensure:

- The processing is truly necessary
- The data is kept secure

To process sensitive data, we need one of the legal bases listed above for non-sensitive data **and o**ne of the following additional legal bases:

- The individual has given explicit consent
- It's required under employment, social security, or social protection laws
- It's needed to protect someone's life or health when they can't give consent
- The individual has made the data public
- It's necessary for legal claims or court proceedings
- t's for a substantial public interest, backed by law, and respects individuals' rights
- It's for medical treatment or health/social care services by professionals
- It's for public health reasons

All sensitive data must be handled according to the **Policy for Processing Special Categories of Personal Data and Criminal Offence Data**.

Criminal Convictions Data

There are special rules for handling data about criminal convictions or offences. This type of data must also follow the **Policy for Processing Special Categories of Personal Data and Criminal Offence Data**. If you're unsure, ask the **Data Protection Officer** for guidance.

Consent

What is Consent?

Consent means a person clearly agrees - freely, specifically, and knowingly - to the use of their personal data, either through a statement or a clear action.

Genuine Choice and Control

Consent must give people real choice and control. If someone feels pressured or can't say no without negative consequences, the consent isn't valid. People must be able to:

- Refuse consent without penalty
- Withdraw consent easily at any time

Consent should be kept separate from other terms and conditions, with clear options for different types of data use.

When Consent Is Needed

Consent is one legal basis for processing personal data, but it's not always required. If another legal basis applies, consent may not be necessary. When consent is needed:

- Individuals must be clearly informed
- Their decision must be respected
- A written record must be kept for auditing

How CareTech Uses Consent

We will only ask for consent when individuals truly have a choice. If another legal basis is more appropriate, we will use that instead.

Use of Personal Data in Media

Personal data or photos will not appear in newsletters, websites, or other media without consent.
Consent will also be requested before displaying personal information (like certificates) in our Locations.
Routine consents will be included in care data forms to avoid repeated requests.

Public Information

Consent is not needed to publish information that's already public, such as staff details in bulletins or parent newsletters. Employees who want to withdraw consent for this should contact the **Human Resource Director**.

If Someone Can't Consent

If a person is unable to give consent, a **'best interest' assessment** must be carried out to guide the decision.

Children

Communications directed at children and young people must be easy to understand. They should be appropriate for the child's age and designed in a way that appeals to younger audiences. If we use consent as the legal basis for handling a child's personal information, we will get consent directly from children aged 13 and older. For children under 13, we will seek consent from the person who has parental responsibility. In cases where parents are separated or the child cannot give consent themselves, decisions should be made based on what is in the child's best interests.

Direct Marketing

Direct marketing refers to any form of advertising or promotional communication that is sent directly to individuals. CareTech will only engage in direct marketing if one of the following applies:

- The individual has given clear, explicit consent
- There is a legitimate business reason, and advice has been sought from the Data Protection Officer

Even when consent or a legitimate interest is in place, all marketing messages, whether by email, web, or other means, must include an option for individuals to opt out. Individuals must be given the chance to opt in to receive marketing materials when their data is first collected. If third-party marketing materials are being sent to named individuals, proper opt-in systems must be in place. If this isn't possible, the materials must not be sent.

Data Security and Retention

To keep personal data safe, CareTech must take steps to prevent physical loss or damage, and limit access and sharing to authorised individuals only. All staff are responsible for:

- Keeping personal data secure
- Not sharing personal information with unauthorised people, either verbally or in writing
- Ensuring computer screens in admin areas are not visible to passers-by and are never left unattended while logged in
- Storing paper records securely and out of sight from anyone without permission to view them
- Taking extra care to protect sensitive personal data from unauthorised access.

The Head of Location or Service Manager is responsible for making sure that only those who need access to data for their job can view or use it. CareTech will keep personal data while individuals are receiving services or are employed, and for a period afterward, in line with legal timeframes and our Data Retention Schedule. Staff must ensure that data is not kept longer than necessary.

Right to Access Information

Employees and anyone whose personal data is held by CareTech have the right to access that data. This includes both electronic records and certain paper-based files stored in manual systems.
In some cases, individuals also have the following rights:

- To be informed about what data is collected and how it's used
- To access their personal data
- To request corrections to inaccurate data

- To request that their data be deleted
- To limit how their data is used
- To transfer their data to another person or organization
- To object to how their data is being processed
- To avoid being subject to automated decisions or profiling

These rights may have exceptions, as outlined in the UK GDPR and the Data Protection Act 2018. Any requests must follow CareTech's Access to Records policy, and staff should seek advice from the Data Protection Officer when needed. All questions or concerns about personal data must be handled quickly and respectfully.

Data Disclosures

Personal data will only be shared with:

- People or organisations who have the individual's consent
- Organisations that have a legal right to access the data without needing consent

If someone requests data over the phone, CareTech must confirm they are authorised and verify their identity—ideally by calling them back through a switchboard to reduce the risk of fraud.
If the request is made in person, CareTech must confirm the person's identity and their right to access the data. If they're not known to staff, proof of identity must be provided.

Police Officers can only access personal data if they provide formal written documentation showing a legitimate need—such as a Schedule 2 request under the Data Protection Act for criminal investigations. Whenever personal data is disclosed, a record must be kept. This helps track what was shared and allows CareTech to notify the recipient if any errors are later found to be inaccurate.

Sharing Information with Partners, Relatives or Carers

When an individual is admitted to a service, hospital, or facility, staff must ask for their consent before sharing any details about their condition or progress with partners, relatives, or carers. If they refuse, this decision must be recorded clearly so that all staff are aware and can respond appropriately to enquiries. If the person is unable to give consent—such as being unconscious or unable to understand—information should only be shared with their next of kin. This is typically a spouse or partner. If they have no partner, their parents and children have equal rights to receive information. If none of these relationships apply, a sibling may be considered. For other relatives, staff should seek guidance from the Multi-Disciplinary Team before sharing any details.

Extra care must be taken when sharing information about people with learning disabilities. In some cases, it may be appropriate to speak with someone who has a formal caring role, but only if it is clearly in their best interest. Any information shared should be limited to what is necessary for the individuals ongoing care.
If the individual is unable to give consent, it is good practice to keep a record of what information was shared and with whom. If the individual later becomes able to give consent, they must be informed about what was shared and asked whether they agree to continue sharing information.

People under the age of 16 have the same right to confidentiality as adults. They must be asked for consent before any information is shared with relatives or carers. If a young person under 16 has the capacity to make decisions about their own treatment, they also have the right to decide whether their personal information can be shared. In such cases, professional staff should be consulted.
Information about an individual —including updates on their condition or future appointments—should not be given over the phone unless the individual has given permission or the caller's identity and right to the information are clearly confirmed. As a general rule, only basic details should be shared. More detailed

information may be given to immediate family members who live far away, but only if staff are confident the person is entitled to it and the individual has not objected.

Photographic, Audio & Video Recordings

Consent is always required before taking any photos, audio, or video recordings. If someone refuses, their decision must be respected. Verbal consent is acceptable and should be recorded in the individual 's notes. If the recordings or images may be published, a written consent form is recommended. Individual s must be told—in a way they can understand—why the recording is being made and how it will be used. Without this explanation, consent is not valid. The person requesting the recording is responsible for obtaining consent. Images taken for care or treatment are confidential. A printed copy should be placed in the individual 's record and protected like any other sensitive document. Once printed, the digital image must be deleted from the device. To protect privacy, people we support, relatives, and visitors should avoid using personal phones or cameras to take photos on CareTech premises.

Use of Social Media

Social media must never be used in ways that go against CareTech policies or compromise confidentiality. Employees and individual s' personal information must always be respected. Defamatory or negative comments about staff, people who use our services, or business partners must not be posted. Employees must not share any content that reveals or hints at the location of children's care services. Anyone posting images or content that breaches confidentiality, includes sensitive or discriminatory material, or identifies a person who uses our services will be held personally responsible.

Removing Individual Records from Company Premises

Individual records must not be taken off-site by staff unless absolutely necessary. Acceptable reasons include:

- Transferring an individual to another service
- Making a home visit that requires access to the individual 's notes
- Providing evidence in a court case when records can't be collected on the day
- Attending a consultation outside the individual 's home or office and needing to update records
- Following work practices that require records to be taken home overnight (they must be returned the next working day).

Transferring Personal Information Abroad

Sharing personal data outside the UK is subject to strict rules. Staff must consult the Data Protection Officer before transferring any personal information to another country.

Personal Information Breach

A personal information breach happens when there's a security failure that leads to:

- Accidental or unlawful destruction of personal data Loss or alteration of personal data
- Unauthorised access to or sharing of personal data
- Any issue involving data that is stored, transmitted, or processed.

If you know or suspect a breach has occurred, report it immediately to your line manager and the Data Protection Officer. You should also take steps to prevent further damage. This might include:

- Making sure an accidentally sent email is deleted by the recipient or access is revoked
- Recovering any lost paper records or devices left in public places
- Changing access codes to buildings that may have been compromised
- Alerting IT if you notice suspicious activity on your device, apps, or network files
- Disconnecting your device from the network and contacting IT directly if you think you're being targeted in a cyber-attack.

To help prevent breaches, all staff must follow the rules in this policy and those outlined in Appendix 2. Handling Personal Information Securely.

This policy must be read in conjunction with the following policies

- CareTech Data Governance Strategy
- Appendix 1 CareTech Data Governance Roadmap
- Information Security
- Risk Management
- Records Management
- Information Systems Acceptable Use
- Access to Records
- Confidentiality Code of Practice
- Processing of Special Category Data and Criminal Offence Data
- Remote Working Policy
- Data Protection Impact Assessments

Monitoring and Review

CareTech will undertake a formal review of this policy if there are any changes to procedure, legislation or regulations.

Revision History

Release Date: September 2022
Review Date September 2025
Next Review September 2027

Signed Russell Edge Russell Edge, Senior Information Risk Owner (SIRO) & Data Protection Officer, Sept 2025

Appendix 1 Roles and Responsibilities
Appendix 2 Handling Personal Information Securely
Appendix 3 Data Protection Policy Terminology