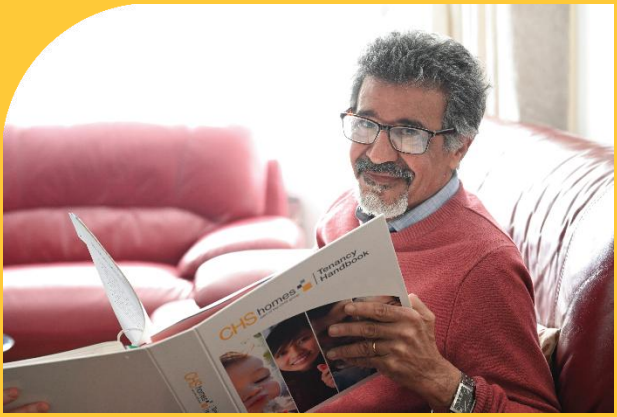
Data Protection Policy



CHS GROUP
housing, care, and community services in Cambridgeshire

Review lead / author name and job title	**Data Protection Advisor**		
Consultation process	Corporate Management Team (CMT) Audit and Risk Committee	**Distribution and training**	Website Synergy Employee Forum Workplace
Last reviewed	February 2024	**Next planned review**	January 2026 (or earlier if legislative changes)
Approved by and date	Board, June 2024		

Change record			
Version no	**Nature of change**	**Last approved**	**Approval**
1	Implementation	June 2011	
2	Full review	January 2015	
3	Implementation of GDPR	August 2018	Audit and Risk Cttee
4	Full review	August 2020	Audit and Risk Cttee
5	Full review	February 2024	Audit and Risk Cttee
6	Change of Cttee	February 2026	Director of Corporate Services

Supporting Policies:

- CCTV Policy (CHS' use of CCTV)
- ICT Security Policy
- Hybrid Working Policy

Supporting Procedures

- Document Retention Guidelines
- Employee Code of Conduct
- Disciplinary Policy and Procedure
- Grievance Policy and Procedure
- Subject Access Request Form and Procedure
- Personal Data Breach Procedure and Incident Response Plan

1. Introduction

1.1 This policy outlines how we set out to comply with data protection legislation, and what we expect of anyone working with personal data on our behalf, to assure individuals that their data is being handled fairly, lawfully, and transparently.

1.2 The core legislation we are referring to in this policy is:

- The Data Protection Act 2018 (DPA) and the
- UK GDPR (the provisions of the EU General Data Protection Regulation having been incorporated into UK law)

2. Purpose and Scope

2.1 This Data Protection policy applies to all the processing of personal data carried out on our behalf by:

- our staff (including permanent, temporary, agency, casual relief, work placement and students)
- board members
- volunteers
- involved tenants with access to personal data
- our data processors, contractors, and agents

2.2 This policy relates to 'personal data', namely any information relating to an identified or identifiable natural living person. NB: some personal data is afforded more protection as it is considered more sensitive, being 'special category' information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric ID data
- Health data
- Sex life and/or sexual orientation
- Criminal data (convictions and offences)

3. Data Protection principles

3.1 Data Protection legislation is guided by six data protection principles, which are reinforced by a seventh principle, namely, to be accountable for compliance with them.

3.2 The six data protection principles require that personal data is:

1. Processed fairly, lawfully and in a transparent manner
2. Used only for limited, specified stated purposes, and not used or disclosed in any way incompatible with those purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate, and where necessary, kept up to date
5. Not kept for longer than necessary, and
6. Kept safe and secure

3.3. We account for our compliance with these principles chiefly by:

- having a Data Protection Policy which outlines our commitment and approach to data protection issues
- having mandatory training for all staff on joining
- giving you access to a range of policies, procedures, and guidance that relate to data protection
- publishing Privacy Notices on our website telling individuals what to expect when we process their personal information, including our lawful reasons and who we'll share data with (and updating these Notices if there are any changes)
- keeping records of our data processing activities, including data sharing agreements and data processing contracts where appropriate
- keeping logs of any data breaches (where data is shared inappropriately, or not kept safe, or not kept available to those who need access), including appropriate actions taken if any breaches are detected
- carrying out risk assessments to assess processing of personal data perceived to be of high risk.

4. Responsibilities

4.1 The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights, and can impose significant penalties for non-compliance with legislation, including major fines, enforcement notices, and criminal prosecutions.

4.2 We take our data protection responsibilities seriously and have an appointed Data Protection Officer (DPO) who is responsible for data protection compliance within CHS. The DPO can be contacted at data.protection@chsgroup.org.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

4.3 We designate our Assistant Director of ICT and Facilities Management as our Senior Information Risk Owner (SIRO) to take overall responsibility for assessing information risk in respect of our organisation. For more information, please see our ICT Security Policy.

4.4 Our Data Protection Officer (DPO)/Data Protection Advisor (DPA) will produce regular reports to the HR & Governance Committee to aid the Board to monitor our compliance with our data protection responsibilities.

4.5 Directors, Assistant Directors, Service Managers and other managerial staff have data protection responsibilities. They will ensure that:

- staff for whom they are responsible participate in appropriate data protection training
- personal information is processed in accordance with the key principles set out above
- they inform the DPO of all actual or potential data protection breaches in their service area as soon as they become aware of the breach
- they inform the DPO of all subject access requests (SARS) made by individuals immediately when they receive one, and assist in any required searches for personal data
- Privacy Notices are available/published covering the processing of personal data within their service area
- records are retained and disposed of in accordance with the relevant retention schedules, which are regularly reviewed, and any changes communicated to staff
- data sharing agreements or data processing contracts are in place, where required, in accordance with corporate guidance
- data protection impact assessments are carried out in accordance with corporate guidance
- data protection audits that will occur periodically shall receive full cooperation and agreed recommendations will be complied with

4.6 You will ensure that:

- personal information is treated in accordance with this and associated policies
- the rights of individuals whose personal data we are processing ('data subjects') are respected at all times
- personal information is only used for the stated purpose, unless explicit consent has been given by the individual to use their information for a different purpose
- personal information is only disclosed on a strict need to know basis to recipients who are entitled to receive that information
- personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities
- personal information is recorded accurately and kept up to date
- you advise your line manager of any individual requests made by data subjects and act in accordance with corporate guidance available
- you raise actual or potential data protection breaches with your line manager and the DPO as soon as the breach is discovered in accordance with corporate guidance available
- records are retained and disposed of in accordance with the agreed retention scheme for their service area.

4.7 It is your responsibility (all those to whom this Policy applies) to ensure that you comply with the requirements of this policy and any associated policies or procedures. Failure to do so may result in the Disciplinary Procedure being invoked for employees and Code of Conduct for Board members.

5. Individual Rights

5.1 We outline below the rights that individuals have in relation to their personal data. Further information is available in our GDPR Factsheets. It is important that advice is sought from the DPO/DPA if an individual requests to exercise their rights (other than simple errors of fact which need rectifying), as not all are automatic, and some can be complex to administer.

5.2 Individuals' personal data rights comprise:

- The right to be informed – we keep individuals informed via our Privacy Notices
- The right of access – **see Point 5.3 below**
- The right to rectification – we must correct inaccurate or incomplete factual information, if the individual can provide evidence to support this
- The right to erasure (the right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

5.3 **The right of access** (often referred to as a 'Subject Access Request' or 'SAR') is particularly important in that there is a tight deadline of **one month** in which to respond, and the process to do so is complex, involving decisions about what data each person is entitled to and what may be withheld. Individuals can make a request to access their data in any way they choose – by phone, by post, electronically, and they may use a different term than 'SAR'. It is very important that, if you recognise that an access request has been received, you alert the DPO/DPA immediately. The DPO/DPA will advise on the next steps in the process. More information is to be found in our Guidance Note on SARs.

6. Lawful basis for collecting Information (Personal Data)

6.1 Data Protection legislation applies to personal data that is "processed". This includes obtaining personal data, retaining and using it, allowing it to be accessed, disclosing it, storing it and, finally, disposing of it. At least one of the following lawful reasons must apply for processing of personal data and must be specified in the relevant Privacy Notice. We list below the lawful reasons in outline – please refer to our Factsheets for more information on each one.

- Consent - an individual has given clear, informed, consent for us to process their data for specific purpose(s). Must be given freely, specific, informed and documented.
- Contract - e.g. to supply goods or services to individuals, employment contracts
- Legal Obligation – e.g. if we are required by law to process the data for a particular purpose - apart from contracts
- Vital Interests – e.g. to protect someone's life
- Public task – to perform a task in the public interest, with a clear basis in law
- Legitimate interests - processing is necessary for our legitimate interests or those of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6.2 Additionally, the 'special categories' of sensitive personal data listed at 2.2 of this Policy can only be processed if at least one further condition is met. These are to be found in our Factsheet about processing special category or sensitive data and must be identified in our Privacy Notices.

6.3 We will only process personal information if we have a business need to do so and we can identify the lawful grounds and, where appropriate, the special conditions for doing so.

6.4 We will specify in our Privacy Notices where we may obtain personal data from, (if not direct from the individual) together with the reasons for doing so and whether consent will be required.

7. Data security considerations

7.1 All those processing data on our behalf to whom this policy applies must ensure that any personal information which they hold is kept secure and that they take appropriate security precautions, by following the terms of our ICT Security Policy regarding computerised data and ensuring any hard copy personal data is kept in locked cabinets or drawers.

7.2 Key ICT security principles include:

- Security and confidentiality in storage and/or transmission of personal data is paramount, and no confidential or sensitive information will be kept in open folders, files, or locations
- Access to all data requires login using multi-factor authentication
- Data kept secure by using multi-layer backup including offsite web-based immutable backup
- access to a knowledge management system (Synergy) where data may be shared using secure links; if emails must be used to transmit personal records, then password-protection or encryption of personal data must be in place
- Microsoft hosted email which is end-to-end encrypted
- Personal information should be stored in the system designed for it (e.g. tenant information in housing management system)
- Individual passwords are kept confidential and not disclosed to others
- Logged on PCs are not left unattended where data is visible on screen
- Inactive computers are automatically logged out.

7.3 When manual records are no longer required, they should be shredded or placed in confidential waste bins so that they are disposed of securely.

7.4 Off-site use of personal data presents a greater risk of loss, theft or damage, and organisational and personal liabilities increase accordingly. For these reasons all those to whom this Policy applies should:

- Only take personal data off-site when authorised to do so and it is absolutely necessary and for the shortest possible time
- Take particular care when laptops or personal machines are used to process personal data at home or in locations outside of CHS, and they are kept secure at all times. Line managers should approve the use of remote working technology in advance of remote working taking place
- Not store personal data on local drives or on personal devices that are used for work purposes
- Where laptops/tablets or other devices are taken off site, you must follow our relevant policies relating to the security of information and the use of computers for working at home/using your own device to work
- Where records are taken off site, you must ensure they do not leave your laptop, other device, or any hard copies of these records on the train, in the car or any other public place

- You must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

8. Data Protection Impact Assessments (DPIA)

Some processing of personal data may result in risks to privacy. Where processing might result in a high risk to individual's rights and freedoms, we will carry out a Data Protection Impact Assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

9. Passing information to other organisations

9.1 Personal data will only be passed to other organisations on a need-to-know basis and with an individual's consent unless there are exceptional circumstances. Exceptional circumstances include:

- Where there is evidence of fraud
- To comply with the law
- In connection with legal proceedings and/or in connection with investigations into potential criminal activities
- Where it would be essential to enable us to carry out our duties, e.g. where the health and safety of and individual would be at risk by not disclosing the information or where there is a legal requirement to do so anonymously for statistical or research purposes
- Where we have a Data Sharing Agreement in place with an external organisation and the data subject has been made aware of this agreement through the provision of a Privacy Notice.
- Where we are required by law to provide information.

Where information is shared with other organisations, we (CHS and our employees acting on our behalf), will comply with all legal requirements of this policy and ensure adequate protection of the information shared.

9.2 We will not transfer personal data to countries outside of the European Economic Area (EEA) and we have obtained assurance from all suppliers that they also do not store or transfer data outside of the EEA.

10. Disposal

10.1 Information should be disposed of in line with the relevant retention schedule.

Where information is disposed of, you should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in your inbox or trash folder. Hard copies of information may need to be confidentially

shredded. You should be careful to ensure that information is disposed of in the confidential waste bins provided as per the shredding process.

10.2 If anyone to whom this Policy applies acquires any personal information in error by whatever means, you shall inform your line manager immediately and arrange for the incident to be handled by the appropriate individual within the organisation, following the Data Breach Incident Response plan.

11. Security

11.1 We take the security of personal data seriously. We have policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by individuals in the proper performance of their duties.

11.2 Role based levels of security

- Our ICT systems will restrict records access to only those employees who require the information to work
- Security access will be reviewed when/if you change job and amended appropriately. System access will be removed the same day when you leave an organisation. If you are suspended or dismissed system access will be removed the same day.

11.3 Encryption - Portable devices that store personal data (for example laptops, USB sticks, DVD/CD media, work mobile phones) pose a high risk to data security. You must only use encrypted devices, appropriate passwords and/or two factor authentication for your work activity.

11.4 Any employee handling personal data must ensure that this information remains confidential and secure; failure to do so may result in disciplinary action.

11.5 Where we engage third parties to process personal data on our behalf, such parties do so on the basis of written instructions (data sharing agreements or data processing contracts), are under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

12. Administration in respect of this policy

12.1 All customers, employees and Board members will be informed of this policy.

12.2 Employees who process data will receive training on data protection legislation.

12.3 Any complaints of breaches of the policy should be reported using our normal complaints procedure for customers and Grievance procedure for employees. Breaches of the policy will be dealt with in accordance with our policies and procedures.

12.4 As required by law, we are registered as a data controller (Z6295350) with the ICO.

13. Policy Monitoring and Review

13.1 The policy and procedure on Data Protection will be reviewed every two years to ensure that it is effective and complies with current good practice. A review will be carried out sooner should there be any changes to statutory requirements.

13.2 A record of all breaches of this policy will be maintained by the DPO/DPA. Quarterly monitoring reports covering data breaches, subject access requests and staff training will be presented to the HRG Committee.

14. Consequences of non-compliance

14.1 You are under an obligation to meet your responsibilities set out in this policy when accessing, using, or disposing of personal information. Failure to observe the data protection responsibilities within this policy may result in you incurring personal criminal liability. It may also result in disciplinary action being taken, up to and including dismissal. For example, if you access another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

Appendix: Glossary

Data Protection legislation regulates the use of a data subject's personal data:

- Personal data: Any information that relates to a living individual who can be directly or indirectly identified from the information, whether singularly or by combining with other information available, including name, identification number, location data, online identifiers (IP addresses, cookies) etc. Applies to both automated personal data and to manual filing systems
- Data subject: the **living** individual to whom the personal data relates or who it identifies
- Processing: is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it
- Data Controller: a person or organisation that determines the purpose for which, and the way(s) any personal data are, or are to be, processed
- Data Processor: means a person or organisation who processes the data on behalf of the Data Controller

- Privacy Notice: a statement which provides data subjects with information on the purpose for processing their personal data, retention periods for the personal data and who it will be shared with.

If you require this document in an alternative format such as large print, braille, or a translated version, please contact us on 0300 1113555 or email info@chsgroup.org.uk.

If you are viewing this document on our website, you can translate the content or listen to it by selecting the ReadSpeaker icon located next to the document title on our Policies page.