Data Protection Policy

Job Title	Group Director of Finance
Ratified by forum & date	Finance & Audit Committee, 04 August 2020
Implementation date:	June 2011, Jan 2015, Aug 2018, Aug 2020
Reviewed:	January 2015 June 2017 July 2018 July 2020
Next Review Due:	July 2022

Supporting Policies:

- Mobile Working Policy
- CCTV Policy
- ICT Security Policy

Supporting Procedures

- Data Protection – Document Retention Guidelines
- Confidentiality for Data Holders Guidelines
- Disciplinary Policy and Procedure
- Grievance Policy and Procedure
- QL data protection protocol
- Subject Access Request Form and Procedure
- Social media guidelines
- Personal Data Breach Procedure and Incident Response Plan
- Guide to CHS Online Services April
- Guidance Note (10) GDPR and Working from Home

1. Introduction

1.1. The Information Commissioner's Office (ICO) is the independent Supervisory Authority responsible for upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The legislation currently relevant to data protection includes the EU General Data Protection Regulations (GDPR) and Data Protection Act 2018. The GDPR consists of seven key principles of good information handling that all organisations and individuals processing personal data have to comply with.

2. Purpose and Scope

2.1. CHS has a responsibility under data protection legislation to hold, obtain, record, use and store all personal data relating to an identifiable living individual in a secure and confidential manner. CHS takes its duties seriously and this policy is a statement of what CHS does to ensure its compliance with Data Protection legislation.

2.2. The Data Protection Policy applies to all CHS employees (including permanent, temporary, agency, work placement and contract), Board members, volunteers and other parties, such as involved tenants, who have access to personal data on behalf of CHS. It applies also to our Data Processors, contractors and agents. The policy identifies information that is to be treated as personal data and therefore confidential, and the procedures for collecting, storing, handling and disclosing such information. It covers all records and information held by CHS concerning personal data held in relation to customers, housing and other service applicants, employees, employment applicants and Board members. All individuals have a right to privacy and CHS is bound by Data Protection legislation.

3. Data Protection principles

3.1 Data Protection legislation requires that seven data protection principles be followed in the processing of personal data. These principles require that personal data must be:

a) Processed fairly, lawfully and in a transparent manner;

b) Collected for specified, explicit and legitimate purposes only;

c) Adequate, relevant and limited in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; with all reasonable steps taken to ensure that inaccurate data is rectified or deleted without delay;

e) Not kept for longer than is necessary for the registered purposes;

f) Kept securely and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage;

The seventh data protection principle is an Accountability principle that requires CHS to take responsibility for complying the principles, and to have appropriate processes and records in place to demonstrate compliance.

3.2 CHS details the reasons for processing personal data, how it uses such data and the legal basis for processing in our Data Register and in our Privacy Notices. Privacy Notices are available on the CHS website. CHS will not process personal data of individuals for other reasons. Where we rely on legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

4. Definitions

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

4.1 Data Subject**:** Any **living** individual who is the subject of the personal data (i.e. existing and past customers, existing and past employees, housing applicants, clients receiving support or services regardless of tenure, Board members).

4.2 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.

4.2 Processing: is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

4.3 Special categories of Personal Data: (previously known as sensitive personal data) – Legislation recognises that some data is more sensitive than others, and requires appropriate handling as this type of data could create more significant risk to a person's fundamental rights and freedoms (e.g. putting them at risk of unlawful discrimination) There are special category conditions that must apply before this type of personal data can be lawfully processed. The following are types of Special categories of personal data:

- Race or ethnic origin
- Sexual life or sexual orientation
- Political opinions
- Religious beliefs or other philosophical beliefs
- Physical/ mental health information
- Genetic and biometric data (where used for ID purposes)
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)

4.3 Criminal offence data: Any information about an individual's criminal convictions and offences or related security measures. This data is no longer included as special category data under GDPR. Instead there are separate safeguards set out in the regulations, that require the Data Controller to have appropriate policy documents in place and the processing is necessary for the purposes of performing or exercising obligations or rights under employment law, social security law or the law relating to social protection.

4.4 Data Controller: a person or organisation that determines the purpose for which, and the manner in which, any personal data are, or are to be processed.

4.5 Data Processor: means a person or organisation who processes the data on behalf of the Data Controller.

4.6 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.

5 Responsibilities

5.1 CHS has 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.

5.2 The Board and Management Team will be responsible for ensuring that the organisation complies with its responsibilities under data protection legislation through monitoring activities and incidents via regular reports by the Data Protection Officer to SMG/Finance and Audit Committee.

5.3 All Directors, Heads of Service, Service Managers and other managerial posts will be fully aware of their responsibility with regard to data protection legislation. This will be achieved through inclusion in contracts of employment and job descriptions, coupled with the provision of appropriate awareness training, supported by guidance notes and procedures detailing organisational and individual responsibilities and action required to ensure compliance with the Act. They will ensure that:

- All staff for which they are responsible participate in appropriate data protection training;
- Information is collected and stored in accordance with the seven key principles set out above.
- They inform the Data Protection Officer of all actual or potential data protection breaches in their service area as soon as they become aware of the breach.
- They respond to individual requests (eg subject access requests) in a timely manner and in accordance with corporate guidance on CHSNet/Synergy[1] (under corporate/data protection);
- Privacy notices are available/published covering the processing of personal data within their service area;
- All 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 are in place where required in accordance with corporate guidance on CHSNet/Synergy (under corporate/data protection);
- Data protection impact assessments are carried out in accordance with corporate

[1] CHS Synergy, replaces CHSNet in August 2020 as an internal document management system.

guidance on CHSNet/Synergy (under corporate/data protection);
- Data protection audits that will occur periodically, shall receive full cooperation and agreed recommendations will be complied with.

5.4 All staff will ensure that:

- Personal information is treated in a confidential manner in accordance with this and associated policies;
- The rights of data subjects are respected at all times;
- Personal information is only used for the stated purpose, unless explicit consent has been given by the data subject 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 is kept up to date;
- They advise their line manager of any individual requests made by data subjects and act in accordance with corporate guidance available on CHSNet/Synergy (under corporate/data protection).
- They raise actual or potential data protection breaches with their line manager and the Data Protection Officer as soon as the breach is discovered, using the appropriate form available on CHSNet/Synergy, under corporate/data protection. Serious Breaches may require disclosure to the ICO and data subject within legislative timescales.
- All records are retained and disposed of in accordance with the agreed retention schedule for their service area.

It is the responsibility of all Board members, staff, volunteers and agency workers to ensure that they 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.

6. Individual Rights

6.1 As a data subject, individuals have a number of rights in relation to their personal data:

- The right to be informed
- The right of access
- The right to rectification
- 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

Further information is available to employees about Individual Rights on Factsheet (4) Rights of Individuals (Data Subjects) on CHSNet/Synergy (under corporate/data protection). Not all rights are automatic and therefore it is important that requests are given due consideration and advice obtained where necessary from the DPO before such requests are actioned.

7. Collecting Information (Personal Data)

7.1 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 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:

- Consent (*see factsheet on consent for further information) - An individual has given consent to the processing for one or more specific purposes of their data being processed and used. "Consent" of the data subject means freely given, specific and informed and must be documented.

- Processing is necessary for the performance of a contract - to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. contract to supply goods or services they have requested or fulfil obligations under employment contract);

- Legal Obligation - Processing is necessary for compliance with a legal obligation to which the controller is subject (i.e. required by law to process data for a particular purpose);

- Vital Interests - Processing is necessary to protect the vital interests of the data subject or another natural person (e.g. protect life); generally limited to processing needs for medical emergencies.

- Public functions - Processing is necessary for the performance of a task carried out in the public interests or in the exercise of official authority vested in the controller (e.g. public authority);

- Legitimate interests - Processing is necessary for the performance of a task carried out in the public interest (includes commercial benefit) pursued by the controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7.2 Special categories of personal data cover particular types of personal data (see definition above), and can only be processed if at least one of the following conditions is met in addition to one or more of the lawful grounds set out in paragraph 7.1. The relevant lawful grounds and special conditions must be set out in the Privacy Notice:

- Explicit consent – An individual has given explicit consent that special category personal data can be processed, unless reliance on consent is prohibited by EU Law
- Legal obligation related to employment – The processing necessity for a legal obligation in the field of employment and social security law or for a collective agreement
- Vital interests – The processing of information is necessary in order to protect the vital interests of the data subject or another individual, where the data subject is physically or legally incapable of giving consent. Usually used in a medical situation
- Not for profit bodies – Processing is carried out in the course of a legitimate activity of a not-for-profit body and only relates to members or related persons and the personal data is not disclosed outside that body without

consent

- Public information – Processing relates to personal data which is manifestly made public by the data subject themselves
- Legal claims – Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Substantial public interest – Processing is necessary for reasons of substantial public interest, on the basis of Union or Member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- Healthcare – the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to under vital interests.
- Public health – processing is necessary for public health purposes, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products and medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
- Archive – the processing is necessary for archiving purposes in the public interests, scientific or historical research purposes or statistical purposes and in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measure to safeguard the fundamental rights and the interests of the data subject.

7.3 CHS will only request personal information if it has a business need to do so and it can identify the lawful grounds and where appropriate the special conditions for doing so. If an individual data subject believes a request is not necessary then they may refuse to provide the information, however CHS may not be able to carry out specific work or offer some support without certain personal data being provided..

7.4 CHS might also obtain personal d a t a from organisations that individuals have previously dealt with. Examples are referral agencies / Councils and past landlords in the case of customers, and past employers for employee references in the case of employees and the Disclosure and Barring Service (DBS). Where this is necessary it should be specified in the relevant Privacy Notice, together with the reasons for doing so and whether consent will be required.

7.5 Personal data will be collected at application stage for customers, employees and Board members. Personal data might also be requested whenever either customers or employees communicate with CHS, to enable CHS to carry out their work or access our services. Examples of this would be customers requesting repairs to a property, customers making a complaint about anti-social behaviour, or employees requesting flexible working patterns to suit home lives. Customers, Employees and Board members should be provided with access to the relevant privacy notice at the time of their personal data being obtained by CHS. Privacy Notices are available on the CHS Group website and reference to this should be made in in appropriate application forms/correspondence. For further information about Privacy Notices,

please refer to Guidance Note (1) Privacy Notices on CHSNet/Synergy (under Corporate/Data Protection)

8. Obligations regarding personal data

8.1 CHS is committed to keeping personal data accurate. It is the responsibility of customers, employees and Board members to tell their relevant contact within CHS of any changes to their personal data. The amendment may be required in writing for documentation, depending on the nature of the request.

8.2 All Board members, staff, volunteers and third parties processing data on behalf of CHS must ensure that any personal information which they hold is kept secure and that they take appropriate security precautions by seeking to ensure the following:

- Documents containing personal data are kept in a lockable cabinet or drawer or room;
- Computerised data is password protected;
- Password-protected and encrypted software is used for the transmission and receipt of emails;
- Fax transmissions are avoided, however where no alternative method is available and the use of a fax has been agreed with the recipient, you should contact the recipient before sending the data so that they are available to receive the data and it is not left unattended;
- Data is kept only on encrypted data storage devices supplied by CHS and stored securely;
- Individual passwords are kept confidential and are not disclosed to other personnel
- Logged on PCs are not left unattended where data is visible on screen to unauthorised personnel;
- Screensavers are used at all times;
- Paper-based records are not left where unauthorised personnel can read or gain access to them.

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

8.4 Off-site use of personal data presents a greater risk of loss, theft or damage and the organisational and personal liability that may accrue from the off-site use of personal data is similarly increased. For these reasons staff and others should:

- Only take personal data off-site when you are 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 (via Citrix) at home or in locations outside of CHS, they are kept secure at all times. Line managers should approve the use of Citrix in advance of remote working taking place.
- Personal data must not be stored on local drives or on personal devices that are used for work purposes;
- Where laptops/tablets or other devices are taken off site, employees must follow the organisation's 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, employees must ensure they do not leave their laptop, other device or any hard copies of these records on the train, in the car or

any other public place.

- Employees 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.

9. 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, the organisation 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. For further guidance, please refer to Guidance Note (6)– Data Protection Impact Assessments and templates available on CHSNet/Synergy (under GDPR and Data Protection).

10. Passing information to other organisations

10.1 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 CHS to carry out its duties, e.g. where the health and safety of an 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 CHS has 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 CHS is required by law to provide information

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

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

11. Disposal

11.1 Information should be disposed of in line with the relevant retention schedule. Where information is disposed of, employees should ensure that it is destroyed and a record kept of which files have been disposed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is disposed of in the confidential waste bins provided as per the shredding process.

11.2 If an employee acquires any personal information in error by whatever means, they shall inform their line manager immediately and arrange for it to be handled by the appropriate individual within the organisation, following the Data Breach Incidence

Response plan published on CHSNet/Synergy

12. Security

12.1 CHS takes the security of personal data seriously. CHS has internal 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.

12.2 Role based levels of security

- Our ICT systems will restrict records access to only those employees that require the information to work. For example, someone working in payroll may need to access financial information about staff, but wouldn't need to access sensitive housing records.
- Security access will be reviewed when/if an employee changes job and amended appropriately. System access will be removed the same day when an employee leaves an organisation. If an employee is suspended or dismissed system access will be removed the same day.

12.3 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. Employees must only use encrypted devices and/or appropriate passwords for CHS work activity. CHS supplied mail enabled devices can be wiped remotely if lost or stolen.

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

12.5 Where CHS engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions (data sharing agreements), are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

13. Access to Personal Data process

13.1 Individuals who have personal data stored by CHS have a right to access those details. Should an individual wish to make a request they should be encouraged to write to their usual contact (Housing Officer, Admin Officer or Project Worker for a customer or Line Manager for an employee) or complete a 'Subject Access Request form'. Once a 'written request or completed form has been received, the usual contact should write an acknowledgment letter and provide a full response within 30 days. Further guidance is available on CHSNet/Synergy (under corporate/data protection) and/or from the Data Protection Officer. If the data subject requests the information but does not wish to put their request in writing then, the same process should apply as they are not legally required to put their request in writing.

13.2 An administration fee may only be charged if the request is excessive or repetitive to cover the time and admin resources to put together all the personal data that we hold for an individual.

An individual is entitled to know what information CHS holds about him or her, and to be given a description of:

- The personal data held
- What purposes the data is used for
- Those who have access to the data

- The retention period for storing personal data or, where this is not possible, the criteria for determining how long the data will be stored
- The existence of their rights including their right to complain to the ICO
- The source of the data, where it was not obtained directly from the individual.

13.4 Please note, there are a number of exceptions to the rights of individuals which mean that CHS will not meet a request if:

- Part of the information relates to another individual who has reasonably refused to consent to his or her personal data being disclosed
- A similar request has been recently complied with
- providing the information would involve 'disproportionate effort' by CHS
- The disclosure of the information might affect the individual's physical or mental condition, unless a health professional has been consulted
- The individual's identity has not been confirmed
- The required fee has not been paid (in cases where the request is manifestly unfounded or excessive).
- Disclosure of the data would compromise CHS safeguarding or whistleblowing policies

13.5 CHS guarantees that the service an individual receives will not be adversely affected by their decision to make a subject access request.

13.6 CHS also guarantees that the need to abide by Data Protection legislation will not affect or prevent good practice sharing of records with service users.

14. General Access to other CHS Information

14.1 CHS is committed to be open about sharing Board level information when able to do so and the following guidelines will be applied.

Non-confidential Board and Committee minutes will be published on CHS's website.

Shareholders, Board Members and Tenants, Residents or Customers:- Copies of Board/Committee supporting papers will be made freely available on request, subject to CHS's Data Protection Policy and except where the whole issue is confidential. Papers may be released subject to the deletion of any items of a confidential nature or those which relate to the personal circumstances of any individual. Requests for other information will be considered by the Company Secretary on their merits and in the light of guidance on Freedom of Information requests.

Any other individual or organisation: - Requests for copies of Board/Committee minutes and supporting papers will be considered by the Company Secretary. Copies will be made available wherever possible but subject to the same exclusions. The general approach will be to provide open information. Requests for other information will be considered by the Company Secretary on their merits and in the light of guidance on Freedom of Information requests.

Other non-confidential information

- Useful information for Customers will be placed on the internet. This includes access to MyCHS and our recruitment information via our recruitment pages on our website .
- Employees will have access to internal information via CHSNet/Synergy, Workplace

and other social media. Note employees must not place confidential data and information on Workplace or social media.

15. Training

15.1 CHS provides (compulsory) training on data protection to all employees who handle personal information in the course of their duties at work. CHS will provide employees with refresher training on a regular basis. If an employee considers that he/she would benefit from refresher training, he/she should contact their line manager or Training Co-ordinator, who is part of the HR team

15.2 ICT team members regularly receive Penetration testing and ethical hacker training.

16. Administration in respect of this policy

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

16.2 Employees that process data will be trained to ensure full understanding of the Data Protection legislation.

16.3 Any complaints of breaches of the policy should be reported using CHS's normal complaints procedure for customers and Grievance procedure for employees.
Breaches of the policy will be dealt with in accordance with CHS's policies and procedure with regard to Board members and employees.

The Personal Data breach procedure must be followed as soon as CHS become aware of the breach to establish the facts and associated risks and comply with statutory timescales.

16.4 As required by law, CHS is registered as a data controller (Z6295350) with the ICO, based on payment of an annual data protection fee.

17 Policy Monitoring and Review

17.1 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.

17.2 Breaches of this policy will be recorded. Data breaches and Subject Access Requests will be monitored through quarterly reporting to the Group Audit and Finance Committee.

17.3 The Group Finance Director and/or Data Protection Officer will make an annual statement of compliance.

18. Consequences of non-compliance

18.1 All employees are under an obligation to meet their responsibilities set out in this policy (see above) when accessing, using or disposing of personal information. Failure to observe the data protection responsibilities within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action being taken, up to and including dismissal. For example, if an employee accesses 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.