DATA PROTECTION POLICY

call 01452 424344
email customer.experience@gch.co.uk
visit www.gch.co.uk

Pride. Quality. Integrity. Innovation.

Business Information provided by Gloucester City Homes

DATA PROTECTION POLICY

DOCUMENTATION MASTER SHEET

Amendments to this Document are Detailed Below.

Version Number	Date Amended	Comments	Date Approved	Author	Approved By
01	02/12/2015	Initial version – replaces Access to Information Policy	N/a	ECR	N/a
02	08/03/2016	Reviewed with Data Protection working group	25/05/2016	ECR/FH /AP	Resources Committee
03	23/08/2018	Updated references to DPA 2018	N/a	PDM	N/a
04	22/10/2018	Updated due to DPA2018		ARR (GCH DPO)	
05	31/10/2018	Resources Committee Update	31/10/2018	ARR (GCH DPO)	Resources Committee
06	05/03/2019	Template change and style update		ARR (GCH DPO)	PM
07	21/05/2020	Reviewed and no changes required	21/05/2020	ARR (GCH DPO)	N/A
08	01/09/2021	CCTV section added & Minor adjustments for clarity made.	29/10/2021	ARR (GCH DPO)	Audit & Risk Committee
09	16/02/2023	Complete re-write of Policy with support from Data Protection People	12/07/2023	DPO & DPP	ELT
10	25/10/2024	Updated wording to different processes and titles	07/11/2024	ASa & RA	ELT

DATA PROTECTION POLICY

CONTENTS

Documentation Master Sheet 2
1. OVERALL AIM 5
2. SCOPE OF POLICY 5
3. RESPONSIBILITIES 6
3.1 Data Controller 6
3.2 Chief Executive Officer 6
3.3 Management and supervisory staff 6
3.4 Data Protection Officer 6
3.5 Process Owners 6
3.7 HR Management 7
3.8 IT Management 7
3.9 Employees, volunteers, temporary workers, directors and officers etc 7
3.10 Partner & Third-Party Responsibilities 8
4. LEGAL AND REGULATORY EXPECTATIONS 8
4.1 Data Protection Officer (DPO) 8
4.2 Fair Lawful and Transparent processing 8
4.3 Data processing purposes 9
4.4 Data minimisation 9
4.5 Data accuracy 9
4.6 Data retention 9
4.7 Information security 10
4.8 Children's data 10
4.9 Personal data relating to criminal convictions and offences 10
4.10 Special categories of personal data 10
4.11 Consent Policy 11
4.12 Record keeping and accountability 11
4.13 Information rights policy 12
4.14 Personal Data Breaches policy 12
4.15 Data Processors 13
4.16 The organisation as a data processor 13
4.17 Data sharing, disclosure and transfer 13
4.18 Internationalisation of personal data 14
4.19 Risk assessment 14
4.20 Training and awareness 15

4.21 Continuous Improvement, audit and compliance checking 15
4.22 Data protection by design and by default 15
5. REVIEW 15

1. OVERALL AIM

This Data Protection Policy sets out the organisation's commitment and approach to data protection and provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance. The policy's objectives are:

- To provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance;
- To provide information to data subjects, data processors, and the regulatory authorities about how the organisation approaches data protection compliance;

Unless otherwise stated this document applies to all **personal data** processed by Gloucester City Homes (GCH). It applies to any natural or legal person who we process personal data for or on behalf of GCH including: employees, volunteers, casual and temporary employees, directors and officers, external organisations employed as processors and any external organisations or individuals with whom GCH shares or discloses personal data. It also applies where GCH is a joint controller or where relevant, acts as a processor for another controller.

2. SCOPE OF POLICY

GCH is committed to compliance with all relevant Data Protection Legislation. The organisation will maintain a suite of policy documents setting out how it intends to implement management controls sufficient to ensure legal compliance with Data Protection Legislation and will ensure that these documents are reviewed periodically to a) test their adequacy in meeting the legal standards as they change over time, and b) to test the organisation's compliance with them.

The organisation will ensure that all relevant personnel and/or other persons it commissions to process personal data on its behalf, either directly or indirectly, have received appropriate and sufficient training in the application of the organisation's policies.

GCH will ensure that sufficient and appropriate resources are available to provide assurance that the organisation meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies.

GCH will ensure that the organisation works within the 7 data protection principles and that it implements sufficient controls to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

GCH will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. It will ensure that those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights.

This policy applies to all of the organisation's activities or operations which involve the processing of personal data.

3. RESPONSIBILITIES

3.1 Data Controller

GCH is the legal data controller under the Data Protection Legislation.

3.2 Chief Executive Officer

The Chief Executive is the accountable officer responsible for the management of the organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to the organisation being able to operate.

3.3 Leaders and Line Managers

Each Director, in their respective areas of responsibility, must ensure that all staff members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. Each Director must ensure this policy is adhered to.

Senior Leaders, Operational Managers and Line Managers are responsible for ensuring that all data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

3.4 Data Protection Officer

The organisation will nominate a Data Protection Officer (DPO) who will be responsible for maintaining the policies, guidance and training needed to ensure the organisation is compliant with Data Protection Legislation. The Data Protection Officer will monitor and report to the Senior Leadership Team in respect of compliance, arrange for the investigation of any Data Protection breach incidents, and maintain suitable records of processing activities. They may co-opt other individuals to assist with the management of data protection obligations. The Data Protection Officer will monitor the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporate relevant changes into the Organisation's policy in a change-controlled manner.

3.5 Process Owners

Data processing activities are managed by nominated job roles or individuals. The Senior Leadership Team will ensure that a process owner is assigned to each data processing activity or operation. The Process Owner has primary operational responsibility for compliance with data protection legislation and good practice in respect of assigned processing activities.

Process Owners are responsible for understanding what personal data are used in their business area and how it is used, who has access to it and why. As a result, they are able to understand and address risks to the data and the organisation. Where the nature of the

organisation's activities is such that personal data are processed as part of a single business process across a number of separate hierarchical business units then, responsibility for the business process as a whole may be assigned to one named Process Owner.

The Data Protection Officer will maintain a list of Process Owners and the data processing activities they are responsible for in the ROPA (Records of Processing Activities).

Process Owners may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other HR policies and ensuring that all staff are appropriately trained.

3.6 Governance Groups

The Data Protection Officer is supported in their role by the members of the Strategic Leadership Team, the Programme Board and the Operational Managers.

The Operational Managers apply the data protection principles, policies and procedures in their areas of operation, feeding back issues and concerns to the Data Protection Officer, the Senior Leadership Team and the Programme Board.

The Data Protection Officer attends both the Operational Managers Meetings and the Programme Board and leads discussions on Data Protection at these meetings.

Data Protection Compliance is reported to Board by the Data Protection Officer through the Audit, Risk and Assurance Committee.

3.7 HR Management

The Director of People, Culture and Communications will ensure data protection compliance in relation to the management of the workforce, including recruitment and retention. In liaison with the Data Protection Officer and through the work of the Learning and Development Officer, they will ensure that adequate training is provided to all employees to ensure data protection compliance.

3.8 IT Management

The Director of Data, Systems and Change is responsible for Information Security.

3.9 Employees, volunteers, temporary workers, directors and officers etc.

Anyone who is directly engaged by the organisation to undertake data processing activities including but not limited to employees, volunteers, temporary workers, directors and officers etc. involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking or witnessing should contact the Data Protection Officer. Individuals are expected to complete appropriate training from time to time. Everyone within the Organisation has a duty to comply with relevant data protection policy and legislation and to respect data subjects' rights to confidentiality.

3.10 Partner & Third-Party Responsibilities

Any Third Party or organisation that is commissioned to process data or receives data from GCH or is able to access any personal data which is within the custody of GCH **must** enter into a legally enforceable agreement with the third-party, the nature of which will be determined by the level of involvement with the data that is held/shared/accessed. Any such agreement must be approved by the Data Protection Officer.

This policy applies to anyone who is engaged to process personal data for or on behalf of the organisation including: employees, volunteers, temporary staff, directors and officers, and third parties such as sub-contractors and suppliers, and anyone who the organisation shares or discloses personal data with/to.

4. LEGAL AND REGULATORY EXPECTATIONS

4.1 Data Protection Officer (DPO)

The organisation has determined that it is required to designate a Data Protection Officer and has documented the rationale underpinning its decision which it will keep under periodic review. It will ensure that the DPO's details are recorded on the Register of Fee Payers maintained by the Information Commissioner's Office and will ensure that the contact details of the DPO is provided to data subjects and maintained in other relevant documentation. The DPO will be issued with a job specification formally detailing their key functions and responsibilities.

The Data Protection Officer will promote organisational awareness and compliance with this policy.

4.2 Fair Lawful and Transparent processing

The processing of all personal data by the organisation will only be undertaken in a fair, lawful and transparent manner meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data are being collected and to the people who the data is about if personal data is collected from sources other than the data subject. All privacy information and any changes to privacy information must be approved by the Data Protection Officer.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful basis for the data processing activities intended to be applied to the personal data. The Data Protection Officer is responsible for determining the lawful grounds for processing. Where the lawful grounds are consent, the consent policy will apply. Where the lawful grounds are legitimate interests a legitimate interests assessment (LIA) will be undertaken and documented. Where the lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in the organisation, a public interests assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation will be cited and appropriately documented.

Each Process Owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control, that the consent policy is adhered to, and a LIA/PIA is properly undertaken where necessary. The Data Protection Officer will provide advice regarding lawful processing conditions and maintain a register of the lawful grounds for all of the organisation's processing activities involving the processing of personal data.

Transparency – the organisation will endeavour to provide sufficient information about how personal data is being processed to enable sufficient transparency about its handling of personal data.

4.3 Data processing purposes

Personal data will only be collected, created or otherwise obtained for specific, explicit and legitimate purposes. No data processing will be undertaken or commissioned without the approval of the Data Protection Officer who will maintain a register of data processing activities and their purpose. Process Owners are responsible for ensuring that all of the data processing activities that they undertake and/or commission have been approved by the Data Protection Officer. No personal data will be used for any purpose other than that which it was collected and/or created for without the approval of the Data Protection Officer.

4.4 Data minimisation

The organisation will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that it collects. Process Owners are responsible for ensuring that no un-necessary, irrelevant or unjustifiable personal data are collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The Data Protection Officer will provide advice regarding the justification of personal data collected or created.

4.5 Data accuracy

The organisation recognises that the accuracy of data is important and that some data is more important to keep up to date than others. The organisation will use its reasonable endeavours to maintain data as accurate and up to date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

Process Owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained accurate and up-to-date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up to date are treated appropriately through erasure or anonymisation. The Data Protection Officer will provide advice regarding data accuracy.

4.6 Data retention

The organisation will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymisation.

Process Owners are responsible for determining the retention period for personal data under their control or sphere of influence and the Data Protection Officer will maintain a data retention schedule setting out approved retention periods and end of life treatment. The retention periods for personal data must be approved by the Data Protection Officer. Because data retention is a vitally important issue as both the over-retention and under-retention of personal data could have a detrimental impact on both the data subject and the organisation the Data Protection Officer will undertake periodic data retention audits.

4.7 Information security

The organisation will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In particular, matters of information security are embedded within the ICT Security & Acceptable Use Policy. The Director of Data, Systems and Change will be responsible for this policy and will consult the Data Protection Officer in regard to it. The Data Protection Officer is authorised to challenge the policy and is required to report any concerns to the Board of directors that they may have about it. Regular security tests and checks are also carried out in line with all relevant GCH policies and procedures concerning ICT security.

4.8 Children's data

Special measures will be taken by the organisation if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests. These special measures will be set out in a policy relating to children's data.

If the organisation provides information society services (digital services) that might the used by people under the age of 18, the **Data Protection Officer** will consider the applicability of the Age-Appropriate Design Code of Practice and make provisions accordingly.

4.9 Personal data relating to criminal convictions and offences

If the organisation is processing personal data relating to criminal convictions and offences, it will implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

4.10 Special categories of personal data

Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The organisation will not process special categories of personal data unless it is necessary. Where the processing of special categories of personal data is necessary, the Data Protection Officer will ensure that the lawful grounds for such processing are documented and will maintain a periodic review of the necessity to processing the special categories of personal data.

4.11 Consent Policy

The organisation will interpret consent to be as defined in the GDPR and that any consent will not be valid unless:

- there is a genuine choice of whether or not to consent;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent;

The organisation recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. The organisation recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

Where consent is the lawful basis for processing, the Data Protection Officer will ensure that consent is properly obtained in accordance with the conditions above.

4.12 Record keeping and accountability

In order to fulfil its responsibility to be able to demonstrate compliance with Data Protection Legislation as well as in support of the policy on transparency, the organisation will maintain records of the processing activities that it controls, undertakes or otherwise commissions ("RoPAs") as required by the Data Protection Legislation and specifically those required in Article 30 of the GDPR.

The Data Protection Officer will be responsible for maintaining the RoPAs and providing them to the Information Commissioner's Office on demand as required.

The organisation will strive to maintain additional documentation capable of demonstrating accountability as necessary: the Data Protection Officer will be responsible for determining what records should be kept, for how long and in what format in order to support its accountability.

4.13 Information rights policy

The organisation recognises the legal rights of those whose data it is processing or intends to process and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that the organisation is able to recognise information rights requests and handle them appropriately when they are exercised. These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data and the right to a judicial remedy and compensation

The Data Protection Officer will maintain a procedure setting out how information rights requests are to be handled and ensure that all relevant people are made aware of it.

4.14 Personal Data Breaches policy

The organisation will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of the policy.

All employees and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach. The organisation will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The Data Breach Reporting Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

The Data Protection Officer will be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

4.15 Data Processors

The organisation reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors may be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation.

People wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The Data Protection Officer will provide advice and guidance in respect of this.

A written agreement will be implemented between the organisation and the data processor which at least meets the requirements of the Data Protection Legislation. The Data Protection Officer will ensure that a register of such agreements/arrangements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

No employee is permitted to commission or appoint a third party to process data on behalf of the organisation without adhering to this policy. The Data Protection Officer will maintain operational instructions on the steps to take to appoint a data processor.

4.16 The organisation as a data processor

Where the organisation acts as a data processor it will ensure it retains records of processing activities which record at least the information required under Article 30(2) of the GDPR for each controller it acts on behalf of. The organisation will ensure that it has an appropriate agreement in place with each data controller and will ensure that its employees, volunteers, staff and contractors, receive appropriate training to enable them to ensure compliance with the instructions and contractual terms of each data controller.

The Data Protection Officer will implement measures to ensure that this policy is complied with.

4.17 Data sharing, disclosure and transfer

The organisation will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place. Data sharing agreements must be approved by the Data Protection Officer who will maintain a register of all such agreements. Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data. This policy extends to appointing others to process personal data on our behalf, sharing personal data with organisations, and providing information to ad-hoc requests for information such as those which may be received from the police and other authorities.

The organisation will provide information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Employees are expected to observe the organisation's data transfer policy and to use safe and secure methods of data transfer. Further advice about secure data transfers can be obtained from the IT department.

The Data Protection Officer will implement measures to ensure that this policy is complied with.

4.18 Internationalisation of personal data

The organisation will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by the Data Protection Officer and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK Government;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has a decision with regard the adequacy of its data protection regime (Adequacy Regulations) issued by the UK Government;
- The transfer is made under the unaltered terms of an International Data Transfer Agreement ("IDTA") issued by the Information Commissioner for such purposes and where required a Transfer Risk Assessment ("TRA") issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the UK Government;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

Where necessary the Data Protection Officer will ensure that a risk assessment is carried out on any third country the organisation intends to transfer personal data to and that any supplementary measures are implemented as necessary to ensure adequate protection of personal data.

The Data Protection Officer will implement measures to ensure that this policy is complied with.

4.19 Risk assessment

The organisation will adopt a risk-based approach to processing personal data ensuring that it assesses any risks to privacy or to the rights and freedoms of people before commencing or commissioning or changing data processing activities. Where necessary it will, as a minimum, ensure that a data protection impact assessment is undertaken where required by Data Protection Legislation and/or when one is deemed to be desirable by the Data Protection Officer.

The organisation will maintain a procedure setting out how data protection impact assessments are to be carried out and documented and ensure that appropriate resources are available to advise on DPIAs.

The Data Protection Officer is responsible for maintaining a register of data protection impact assessments that have been undertaken by the organisation and for its periodic review.

4.20 Training and awareness

The Organisation will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies, procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically. Process Owners will determine the training needs of those people within their sphere of control and that appropriate data protection awareness and training is provided, measured and reported.

The Data Protection Officer will implement measures to ensure that this policy is complied with.

4.21 Continuous Improvement, audit and compliance checking

The organisation will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where no-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The Audit, Risk & Assurance Committee will be provided with a summary of audit findings periodically.

The Data Protection Officer will implement measures to ensure that this policy is complied with.

4.22 Data protection by design and by default

The organisation will strive to foster a culture of data protection by design and by default in all of its data processing activities. It will ensure that measures are in place to encourage all those involved in data processing activities to adopt a model of continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into processing activities. The organisation will strive to ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed and that the extent of the processing, period of their storage and their accessibility. In particular, such measures will ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The Data Protection Officer will implement measures to ensure that this policy is complied with.

5. REVIEW

This policy will normally be reviewed triennially to ensure that it reminds fit for purpose, unless an earlier review is required due to regulatory, statutory or other requirements.