Document Name:	Data Protection Policy
Document Type:	Group Policy

Version Date:	March 2022	**Review Date:**	March 2025
Department:	Business Assurance Team	**Document Author:**	Head of Business Assurance

Code for Approval Route:	Board
Approval Date:	10th March 2022
Who has been consulted:	SMT, ELT
Equality Assessment Completed:	Yes

Document Information

Scope:
This policy relates to Community Gateway (CGA) internal procedures and systems for processing individuals' personal data in accordance with relevant Data Protection legislation including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This Policy applies to all CGA Group colleagues, including where appropriate, consultants, Board/Committee members and contractors (Third Parties) who process personal data on our behalf and in accordance with our instructions.

This policy applies to individual personal data and special category personal data held either manually or within electronic systems that are engaged in the processing of such data.

The policy outlines CGA's commitment to comply with all relevant Data Protection legislation and serves to ensure that individuals' rights are protected and upheld.

Key Objectives:
To set out how CGA will meet the requirements of GDPR and the Data Protection Act 2018.

Links to Regulatory Framework for Social Housing
Governance and Financial Viability Standard 2015
"Registered providers shall ensure effective governance arrangements that deliver their aims, objectives and intended outcomes for tenants and potential tenants in an effective, transparent and accountable manner. Governance arrangements shall ensure registered providers:

Document Information
(a) adhere to all relevant law (b) comply with their governing documents and all regulatory requirements (c) are accountable to tenants, the regulator and relevant stakeholders (d) safeguard taxpayers' interests and the reputation of the sector (e) have an effective risk management and internal controls assurance framework (f) protect social housing assets"
Links to Strategic Objectives/CGA Values: Processing personal data in accordance with relevant laws and statutory guidance will underpin the achievement of all CGA's Corporate Objectives but is particularly relevant to the following Corporate Objectives: Invest – Technology and Evolve – Ways of Working.
Retention Schedule: No personal data will be stored as a result of this policy by the Business Assurance Team. The policy details how the organisation as a whole manages data and CGA's retention schedule and departmental policies and procedures will address retention of data accordingly.
Legal Basis for Processing: Not Applicable
Outcomes for Customers: This policy provides assurance that CGA has the requisite policies, procedures, staff training and awareness in place to effectively meet the requirements of Data Protection legislation.

INTRODUCTION

1. CGA acknowledges that all individuals have the right to expect that appropriate safeguards will be put in place to protect the confidentiality and integrity of their personal data.

2. CGA understands that the consequences of failing to comply with the requirements of Data Protection legislation may result in:

   - Loss of trust by our customers and stakeholders;
   - Significant reputational impact and damage;
   - Enforcement powers and fines being implemented by the Information Commissioner's Office;
   - Criminal and/or civil action;
   - Personal accountability and liability;
   - Organisational accountability and liability;

- Loss of confidence in the integrity of our systems and procedures.

DEFINITIONS

3. There are various terms used within this policy and their definitions are as follows:

- **Personal Data** – any information that relates to an identified or identifiable living subject i.e. staff member, member of the public, customer etc. It will generally include an individual's name, address, phone number, date of birth, place of work, their opinions, opinions about them, location data and online identifiers. The list is not exhaustive and any information that relates to an individual can be Personal Data.

- **Sensitive Personal Data** – This information is referred to as information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health or sex life. Under GDPR, genetic and biometric data are also classified as sensitive data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included as sensitive data, but similar extra safeguards apply to its processing under Article 10 of GDPR.

- **Data Processing** – anything that is done to or with Personal Data (including collection, recording, organising, structuring, storage, adaptation, retrieval, deletion and destruction)

- **Data Controller** – the organisation that determines the purposes and means of processing personal data.

- **Data Processor** – A data processor is responsible for processing data on behalf of a Data Controller.

- **A recipient** - a natural or legal person, public authority, agency or other body to which personal data have been disclosed. The definition includes

controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

DATA PROTECTION PRINCIPLES

4. GDPR contains six key principles which set out the main responsibilities of organisations in relation to data protection. These principles are summarised below and CGA will seek to ensure compliance with these principles at all times:

- **Lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

- **Purpose limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- **Data minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- **Accuracy -** Personal data shall be accurate and, where necessary, kept up to date.

- **Storage limitation** - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Integrity and confidentiality** - Personal data shall be 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.

- **Accountability** – Data controllers shall be responsible for and be able to demonstrate compliance with the GDPR.

COMMITMENT STATEMENT

5. The Data Protection legislation is designed to ensure that data controllers and processors meet their obligations and individuals can exercise their rights in relation to the processing of personal data.

6. CGA will comply with all relevant legislation and ensure all personal data is processed in line with individuals' rights and our obligations as a data controller.

7. CGA will ensure that contracts with data processors are compliant with the legislative requirements. Wherever CGA contracts out services/functions involving living individuals' personal data CGA will ensure, through effective procurement practices, that potential suppliers are able to provide satisfactory evidence and assurance that they fully understand and are able to comply with their duties as a Data Processor under relevant legislation. CGA will also ensure that personal data held in relation to suppliers and their employees is processed in accordance with data protection legislation.

POLICY STATEMENT

8. All staff and, where appropriate, consultants, Board/Committee members, contractors and other third parties engaged to carry out duties on our behalf and under our instructions, will adopt and follow this policy and the requirements of the supporting Information Governance policies, procedures. This information governance framework outlines CGA's core requirements relating to the collection, confidentiality, availability and integrity of our data and is comprised of the following policies and procedures:

   - Information Security Policy;
   - Breach Management Procedure;
   - Records Retention and Disposal Procedure;
   - Subject Access Request Procedure;

- Data Rectification, Restriction Objection and Erasure Procedure;
- Data Portability Procedure;
- Data Protection Impact Assessment form.

PROCESSING OF PERSONAL DATA

9. CGA will only process personal data that has been obtained fairly and lawfully and for a specific, explicit and legitimate purpose(s). CGA will ensure the data is adequate and relevant and limited to what is necessary for those purposes, maintained accurately and not retained for any longer than is necessary.

10. CGA understands that it must identify a valid lawful basis for processing personal data before processing begins. CGA has reviewed the purposes of its processing activities and selected the most appropriate lawful basis (or bases) for each activity. CGA has checked that the processing is necessary for the relevant purpose and is satisfied that there is no other reasonable way to achieve that purpose. Where CGA processes special category data, a condition for processing special category data will be identified and documented as part of the records referred to at Paragraph 9. Similarly, where CGA processes criminal offence data, a condition for processing this data will be identified and documented as part of the records referred to at Paragraph 9.

11. If CGA's purpose for processing changes over time or the Association begins processing for a new purpose as a result of business growth or diversification, CGA will consider whether the processing is compatible with the original purpose for processing the data. If the new purpose is significantly different, CGA will consider whether the processing is fair and transparent. If so, a legal basis for processing the data for the new purpose will be identified and documented and individuals affected will be given information about the new purpose.

12. All staff who process personal or sensitive personal data will be responsible for ensuring that it is used appropriately and kept both secure and confidential, ensuring that at all times they only access and process data that they are authorised to manage on behalf of CGA.

13. CGA is committed to ensuring that all appropriate technical and organisational measures are taken against unauthorised or unlawful processing of data and against the accidental loss, destruction or damage to personal data.

14. CGA will not routinely transfer personal data to jurisdictions outside the European Economic Area (EEA). Should CGA transfer data outside of the EEA, it will only do so if the jurisdiction has a recognised and adequate level of protection for Data Protection purposes. Transferring data outside of the EEA will require approval from the Executive Director of Resources following the completion of relevant Information Governance and Security compliance checks.

INDIVIDUALS' RIGHTS

15. CGA understands that efficiently and effectively enabling individuals to exercise their rights under data protection legislation will help to build trust and confidence in the Association. CGA will ensure that the organisation has policies, procedures and processes in place to fulfil individuals' rights as outlined at Paragraph 8 above.

Right to be Informed

16. CGA understands that a key transparency requirement under GDPR is the right of individuals to be informed about the collection and use of their personal data. CGA will ensure that individuals are provided with the required privacy information, which will include but is not limited to: the identity of CGA as the data controller, the reasons why personal and sensitive personal data is required to be processed, how it will be processed, who it may be shared with, CGA's legal basis for processing the data, the length of time that the information will be retained and contact details for CGA's Data Protection Officer.

17. The privacy information which CGA provides will be concise, transparent, intelligible, easily accessible, and written in clear and plain language. CGA will provide privacy information through privacy notices, with separate privacy notices for customers and colleagues. CGA will ensure that an appropriate level of privacy information is provided at the time personal data is collected from

individuals and that they are made aware of how to access the detailed privacy notice. Privacy Notices will be provided in alternative formats to meet individuals' needs upon request.

Right of Access

18. CGA recognises that individuals have the right to make a written or verbal request for access to their personal information and to be provided with a copy of that information. Any such requests will be handled in accordance with the Subject Access Request Procedure referred to at paragraph 8 above.

Rights to Rectification, Restriction and Erasure

19. GDPR provides individuals with a right to have inaccurate personal data rectified and to request that incomplete data is completed. Any requests for rectification will be handled in accordance with the Data Rectification, Restriction and Erasure Procedure.

20. CGA recognises that GDPR introduces a right for individuals to request that their personal data be erased and that individuals also have the right to request the restriction or suppression of their personal data. CGA understands that these rights are not absolute and only apply in certain circumstances. Any requests for erasure or restriction of processing will be handled in accordance with the Data Rectification, Restriction and Erasure Procedure.

Right to object

21. CGA acknowledges that individuals have the right to object to the processing of their personal data in certain circumstances, including where the data is processed on the grounds of legitimate interests or for direct marketing purposes. Any objections to the processing of an individual's personal data will be handled in accordance with the Right to Object Procedure.

Right to Data Portability

22. GDPR introduces a new right for individuals to obtain and reuse their personal data for their own purposes across different services in a safe and secure way without hindrance to usability. CGA understands that this right applies to personal data an individual has provided to a controller, personal data where processing is based on an individual's consent or for the performance of a contract, or when processing is carried out by automated means. Any data portability requests will be handled in accordance with the Data Portability Procedure referred to at Paragraph 8 above.

Rights related to automated decision making and profiling

23. CGA does not currently undertake any automated decision making or profiling as defined under the provisions of GDPR and recognises that this form of processing is normally classified as high risk. Should CGA consider introducing any form of automated decision making or profiling in the future, the Association will take all necessary steps to ensure compliance with GDPR including undertaking a Data Protection Impact Assessment to fully understand and document the risks to individuals. CGA will also introduce a policy and procedure to govern the automated decision-making processing before any processing commences.

INFORMATION SHARING

24. CGA will only share personal data in accordance with the requirements of data protection legislation and the Information Commissioner's guidance on data sharing. We will abide by the laws and regulations in relation to:

- the right to confidentiality;
- data sharing;
- disclosure rules;
- any Civil and/or Criminal disclosure legal requirements.

25. When sharing data with third party data controllers, CGA will take appropriate steps to ensure that the data sharing is in accordance with the data protection

principles and the obligations of GDPR. CGA will take into account any best practice guidance published by the Information Commissioner's Office in relation to data sharing and utilise data protection impact assessments, information sharing agreements and other mechanisms when deemed appropriate to ensure personal data is adequately protected.

26. CGA will inform individuals of the identity of other parties to whom we may disclose or be required to provide personal data, the circumstances in which this may happen and when any exceptions to this rule may apply. Details of categories of recipients with whom we share data will be published in CGA's Privacy Notices.

27. CGA will comply with all relevant policies and practices when exploring or entering into any acquisition or merger and will ensure that all personal or sensitive personal data is anonymised as part of any evaluation of assets and liability assessments, except as required by law.

ACCOUNTABILITY

28. CGA is committed to maintaining comprehensive but proportionate governance and accountability measures to meet the accountability requirements of GDPR and to uphold the protection of personal data.

29. CGA will ensure that all appropriate technical and organisational measures are taken against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to, personal data. These measures will be regularly reviewed and updated to ensure they remain relevant and fit for purpose and minimise the risk of a data breach occurring. Further information on the security measures which CGA has put in place can be found in the IT Security Policy and the Data Breach Management Procedure.

30. As outlined at paragraph 8 above, CGA has in place an Information Governance Framework which comprises a full suite of policies and procedures to support compliance with legislative requirements.

31. CGA will maintain records of the processing activities which it undertakes, and these records will document all the applicable information required under GDPR. This documentation will be reviewed annually to ensure it remains accurate and up to date and will be made available to the Information Commissioner's Office upon request.

Privacy by Design and Default

32. Privacy by design and default is an approach that promotes privacy and data protection compliance from the outset when developing a policy, process, product, system or project. CGA acknowledges that GDPR places a general obligation on CGA to demonstrate that it has integrated data protection into its activities. CGA will adopt a privacy by design approach in order to meet this obligation, to ensure privacy risks are minimised and to build trust.

33. CGA will implement measures that meet the principles of privacy by design in a number of ways which will include:

- Ensuring that privacy by design is embedded within CGA's project management and risk management frameworks;
- Undertaking Data Privacy Impact Assessments (DPIA's), particularly in relation to potential high-risk data processing activities and for the implementation of new IT systems or processes;
- Utilising encryption or pseudonymisation of data where deemed appropriate to provide an additional layer of protection for personal data;
- Reviewing processes and procedures to minimise the data which CGA processes;
- The inclusion of a Data Protection statement on all policies and procedures;
- Utilise approved codes of conduct and certification schemes to demonstrate compliance where this is deemed relevant and appropriate.

Data Protection Officer

34. CGA will appoint a Data Protection Officer (DPO) who will be responsible for undertaking the tasks outlined below. CGA will also appoint a Deputy Data Protection Officer (Deputy DPO) to assist the DPO in fulfilling these responsibilities and to fulfil the responsibilities of the DPO role in the absence of the DPO (defined as a period of leave or sickness absence).

35. In accordance with the requirements of GDPR, the key tasks which the Data Protection Officer will perform are as follows:

- inform and advise CGA and its staff who carry out processing activities of their obligations under data protection legislation;
- monitor compliance with data protection legislation of CGA's policies in relation to the protection of personal data, including the assignment of responsibilities, awareness raising, and the training of all staff involved in processing personal data;
- provide advice on completion of data protection impact assessments;
- co-operate with the Information Commissioner's Office (ICO) and act as the point of contact for the ICO and undertake prior consultation with the ICO on any processing activities which are identified as high risk following the completion of a DPIA.

36. CGA will support the DPO and Deputy DPO in performing the tasks referred to above and will ensure that:

- the DPO and Deputy DPO are provided with the necessary resources to carry out their tasks, to access personal data and processing operations and to maintain their data protection knowledge;
- the DPO and Deputy DPO are able to carry out their role independently and do not receive instruction regarding the exercise of those tasks;
- the DPO and Deputy DPO are not penalised for the performance of those tasks outlined above;
- ensure that the DPO (and Deputy DPO when acting in the capacity of DPO) can report directly to CGA Board on the Association compliance with data protection legislation.

37. CGA's DPO and Deputy DPO will conduct an annual programme of audits to ensure that processing of personal information is being undertaken in accordance with Data Protection legislation and the six principles.

38. The names and contact details of CGA's DPO and Deputy DPO will be clearly stated within CGA's privacy notices.

Staff Responsibilities

39. CGA will ensure that all colleagues understand that they have a responsibility to ensure the organisation complies with legislative requirements in relation to data protection.

40. CGA has provided, and will continue to provide, all colleagues with training on their responsibilities under data protection legislation and will promote awareness of this policy and the associated information governance framework to board members, colleagues, customers and volunteers.

41. CGA has a zero-tolerance policy towards individuals who deliberately and unlawfully obtain or disclose personal data or instructs another person to do so. CGA recognises that this can be an offence under the data protection legislation, which clearly states that any person must not knowingly or recklessly obtain, disclose or procure the disclosure of personal data or instruct another person to do so, without the consent of CGA as the data controller.

42. CGA acknowledges human error can occur; the above relates to a deliberate willful intent to obtain and/or disclose private information for purposes incompatible with a colleagues normal working or operating procedures. In such instances, CGA will take appropriate, proportionate action and, where required, report this to the applicable authorities and regulators.

43. CGA may consider taking internal disciplinary and/or legal action where applicable and lawful where colleagues, consultants, Board/Committee members and/or contractors or third parties, engaged to carry out duties, breach this policy and applicable information governance policies/procedures.

44. CGA shall adhere to legislative requirements when processing personal data in relation to Disclosure and Barring Service checks and will only carry out checks in line with the law for the purpose of employment, money laundering and when there is a public interest requirement.

45. CGA understands a court may grant compensation to an individual if it is found CGA, as the data controller, has infringed the requirements of data protection legislation and as a consequence an individual has suffered material or non-material damage.

46. Complaints relating to alleged breaches of the data protection legislation, or complaints that an individual's personal data is not being processed in line with the data protection principles, will be managed and processed by the Deputy Data Protection Officer. Any subsequent appeal will be considered by the Data Protection Officer unless the Data Protection Officer was involved in considering the original complaint. In such cases, the appeal will be considered by the Executive Director of Resources.

DATA PROTECTION FEE

47. CGA will ensure that it pays the required annual fee to the Information Commissioner's Office in accordance with the Data Protection (Charges and Information) Regulations 2018.

EQUALITY AND DIVERSITY

48. CGA will ensure that this policy, and the supporting policies and procedures that form part of the Information Governance Framework are applied fairly and

consistently. We will not directly or indirectly discriminate against any person or group of people because of their race, religion/faith, gender, disability, age, sexual orientation, gender reassignment, marriage and civil partnerships, pregnancy and maternity or any other grounds set out in our Equality Diversity and Inclusion Strategy.

REVIEW

49. The Business Assurance Team will monitor the effectiveness of this policy and recommend changes to improve compliance with legislative requirements and to implement best practice in the field of data protection and information governance and management.

The Audit and Risk Committee will receive an annual report on CGA's compliance with data protection legislation and a review of this policy will be undertaken every three years.