community gateway

DATA PROTECTION POLICY

REVIEW DATE:
APRIL 2028

Contents

1	Introduction	3
2	Scope of Policy and when to seek advice on data protection compliance	3
3	Personal data protection principles	5
4	Lawfulness, fairness and transparency	5
5	Consent	6
6	Transparency (notifying Data Subjects)	7
7	Purpose limitation	8
8	Data minimisation	8
9	Accuracy	8
10	Storage limitation	9
11	Security, integrity and confidentiality	9
12	Reporting a Personal Data Breach	10
13	Transfer limitation	10
14	Data Subject's rights and requests	11
15	Accountability	12
16	Record keeping	13
17	Training and audit	13
18	Privacy by Design and Data Protection Impact Assessments (DPIAs)	14
19	Automated Processing (including profiling) and Automated Decision-Making	15
20	Direct marketing	16
21	Vulnerability Data	16
22	Sharing Personal Data	16
23	Monitoring and Review of this Data Protection Policy	17
24	Definitions and interpretation	17

1 Introduction

1.1 This Data Protection Policy sets out how Community Gateway Association Ltd and our group companies (referred to as **CGA**, or **we**, **our**, **us**) handle the Personal Data of our tenants, residents, applicants, support workers, trustees, directors, employees, workers, volunteers and other third parties.

1.2 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored and who it relates to.

1.3 This Data Protection Policy applies to all CGA Personnel (**you**, **your**). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and you must also attend training on our requirements in relation to Processing Personal Data. Data protection is the responsibility of everyone within CGA and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable CGA to comply with applicable law. Related Policies are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related Policies. Any breach of this Data Protection Policy may result in disciplinary action.

1.4 Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies.

1.5 This Data Protection Policy (together with Related Policies) is an internal document and cannot be shared with third parties without prior authorisation from the DPO.

1.6 All capitalised terms are defined in section 24 at the end of this Data Protection Policy.

2 Scope of Policy and when to seek advice on data protection compliance

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in CGA and will provide for successful support and services. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. CGA is exposed to potential fines of up to £17.5 million or 4% (four percent) of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the UK GDPR.

2.2 All line managers are responsible for ensuring all CGA Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

2.3 The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies. That post is held by Stephen Pickup, and they can be reached at dataprotection@communitygateway.co.uk.

2.4 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

2.4.1 if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by CGA) (see paragraph 4.1);

2.4.2 if you need to rely on Consent or need to capture Explicit Consent (see paragraph 5);

2.4.3 if you need to draft Privacy Notices (see paragraph 6);

2.4.4 if you are unsure about the retention period for the Personal Data being Processed (see paragraph 10);

2.4.5 if you are unsure what security or other measures you need to implement to protect Personal Data (see paragraph 11.1);

2.4.6 if there has been a Personal Data Breach (paragraph 12);

2.4.7 if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 13);

2.4.8 if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 14);

2.4.9 whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 18) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 7);

2.4.10 if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 19);

2.4.11 if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 20); or

2.4.12 if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see paragraph 21).

3 Personal data protection principles

3.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR, which require Personal Data to be:

3.1.1 Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

3.1.2 collected only for specified, explicit and legitimate purposes (purpose limitation);

3.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

3.1.4 accurate and where necessary kept up to date (accuracy);

3.1.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

3.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

3.1.7 not transferred to another country without appropriate safeguards in place (transfer limitation); and

3.1.8 made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

4 Lawfulness, fairness and transparency

4.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to Data Subjects.

4.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

4.3 The UK GDPR allows Processing for specific purposes, and the relevant purposes are set out below:

4.3.1 the Data Subject has given their Consent;

4.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

4.3.3 to meet our legal compliance obligations;

4.3.4 to protect the Data Subject's vital interests; or

4.3.5 to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden by the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

4.4 We must identify and document the legal ground being relied on for each Processing activity.

5 Consent

5.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

5.2 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

5.3 CGA ensures that its Consent requests are prominent, concise, separate from other terms and conditions, and easy to understand. Consent requests must always include:

- the name of CGA;
- the name of any third party controllers who will rely on the Consent;
- why CGA wants the Personal Data;
- what CGA will do with it; and
- a statement that Data Subjects can withdraw their Consent at any time.

5.4 A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Where Consent has been withdrawn or denied, CGA keeps a record of the withdrawal or refusal, to ensure the Data Subject's choices not to consent are honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.5 When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, we must issue a Privacy Notice to the Data Subject which refers to Explicit Consent.

5.6 We need to evidence Consent captured and keep records of all Consents in accordance with Related Policies, so that CGA can demonstrate compliance with Consent requirements.

5.7 We will establish and implement procedures to securely record, maintain, and track all consents obtained from tenants, including the date, scope, and duration of such consents.

6 Transparency (notifying Data Subjects)

6.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

6.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

6.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

6.4 If we are collecting Personal Data from a Data Subject, directly or indirectly, then we must provide the Data Subject with a Privacy Notice in accordance with our Related Policies.

6.5 You must obtain the approval of the DPO for any new or revised Privacy Notices.

7 Purpose limitation

7.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

7.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

8 Data minimisation

8.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

8.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

8.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the CGA's data retention guidelines.

9 Accuracy

9.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10 Storage limitation

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 We will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. You must comply with our Records Retention and Disposal Policy.

10.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.4 You must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our Data Retention Policy. This includes requiring third parties to delete that data where applicable.

10.5 You must ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined.

11 Security, integrity and confidentiality

11.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.

11.2 We will develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

11.4 You must maintain data security by protecting the confidentiality, integrity, and availability of the Personal Data, defined as follows:

11.4.1 **Confidentiality**: only people who have a need to know and are authorised to use the Personal Data can access it;

11.4.2 **Integrity**: Personal Data is accurate and suitable for the purpose for which it is processed; and

11.4.3 **Availability**: authorised users are able to access the Personal Data when they need it for authorised purposes.

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

12 Reporting a Personal Data Breach

12.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

12.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

12.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the IT helpdesk and follow CGA's Data Breach Management Procedure. You should preserve all evidence relating to the potential Personal Data Breach.

13 Transfer limitation

13.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. A transfer of Personal Data occurs when you transmit, send, view or access that data in or to a different country.

13.2 You may only transfer Personal Data outside the UK if one of the following conditions applies:

13.2.1 the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

13.2.2 appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

13.2.3 the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

13.2.4 another transfer condition is met in the UK GDPR. It is unlikely that we will transfer any Personal Data outside the UK unless we have met the condition in 13.2.1 or 13.2.2. For more information, please contact the DPO.

14 Data Subject's rights and requests

14.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

14.1.1 withdraw Consent to Processing at any time;

14.1.2 receive certain information about the Controller's Processing activities; and

14.1.3 request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

14.1.4 prevent our use of their Personal Data for direct marketing purposes;

14.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

14.1.6 restrict Processing in specific circumstances;

14.1.7 object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

14.1.8 request a copy of an agreement under which Personal Data is transferred outside of the UK;

14.1.9 object to decisions based solely on Automated Processing, including profiling (ADM);

14.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

14.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

14.1.12 make a complaint to the supervisory authority; and

14.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

14.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

14.3 You must immediately forward any Data Subject request you receive to the Business Assurance Team at dataprotection@communitygateway.co.uk.

14.4 Our procedure for dealing with Data Subject access requests is set out in our Subject Access Request Policy and our Subject Access Request Procedure.

14.5 Our procedures for dealing with other Data Subjects rights requests are set out in our Data Rectification, Restriction, Erasure and Objection Procedure and our Data Portability Procedure.

15 Accountability

15.1 CGA must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. CGA is responsible for, and must be able to demonstrate, compliance with the data protection principles.

15.2 CGA must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

15.2.1 appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

15.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

15.2.3 integrating data protection into internal documents including this Data Protection Policy, Related Policies, or Privacy Notices;

15.2.4 regularly training CGA Personnel on the UK GDPR, this Data Protection Policy, Related Policies, and data protection matters including, for example, Data Subjects' rights, Consent, legal basis, DPIAs and Personal Data Breaches. CGA must maintain a record of training attendance by CGA Personnel; and

15.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

16 Record keeping

16.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

16.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

16.3 These records should include, at a minimum:

16.3.1 the name and contact details of the Controller; and

16.3.2 clear descriptions of:

i the Personal Data types;

ii the Data Subject types;

iii the Processing activities;

iv the Processing purposes;

v the third-party recipients of the Personal Data;

vi the Personal Data storage locations;

vii the Personal Data transfers;

viii the Personal Data's retention period; and

ix the security measures in place.

16.4 To create the records, records of processing activities should be created which should include the detail set out above in accordance with our Records Retention and Disposal Procedure.

17 Training and audit

17.1 We are required to ensure all CGA Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

17.2 You must undergo all mandatory data privacy-related training and Business Managers are responsible for ensuring their teams undertake all mandatory training.

17.3 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18 Privacy by Design and Data Protection Impact Assessments (DPIAs)

18.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

18.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

18.2.1 the state of the art;

18.2.2 the cost of implementation;

18.2.3 the nature, scope, context and purposes of Processing; and

18.2.4 the risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

18.3 We must also conduct a DPIA in respect to high-risk Processing.

18.4 We should conduct a DPIA (and discuss any findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

18.4.1 use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes);

18.4.2 automated Processing including profiling and ADM;

18.4.3 large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

18.4.4 large-scale, systematic monitoring of a publicly accessible area.

18.5 A DPIA must include:

18.5.1 a description of the Processing, its purposes and our legitimate interests if appropriate;

18.5.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

18.5.3 an assessment of the risk to individuals; and

18.5.4 the risk mitigation measures in place and demonstration of compliance.

19 Automated Processing (including profiling) and Automated Decision-Making

19.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

19.1.1 a Data Subject has Explicitly Consented;

19.1.2 the Processing is authorised by law; or

19.1.3 the Processing is necessary for the performance of or entering into a contract.

19.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds 19.1.2 or 19.1.3 will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

19.3 If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

19.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

19.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

20 Direct marketing

20.1 Whilst we do not regularly undertake any direct marketing, please note the contents of this section if we are to undertake any (such as emailing tenants with details of any additional services we or any third party can offer).

20.2 The Consent of Data Subjects is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows CGA to send marketing texts or emails without consent if it:

20.2.1 has obtained contact details in the course of a sale to that person;

20.2.2 is marketing similar products or services; and

20.2.3 gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.

20.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. Please refer to our Privacy Notice.

20.4 A Data Subject's objection to direct marketing must always be promptly honoured. If an individual opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

20.5 You must consult the DPO if you are unsure regarding how to comply with either CGA's guidelines or the law.

21 Vulnerability Data

21.1 Where Community Gateway Association Ltd is processing personal data or special categories of personal data relating to vulnerabilities of individuals, all colleagues and individuals with access to this data shall comply with the Vulnerability Data Policy set out at Appendix 1 of this Data Protection Policy.

22 Sharing Personal Data

22.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 You may only share the Personal Data we hold about any individual with another staff member if the recipient has a job-related need to know the information.

22.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

22.3.1 they have a need to know the information for the purposes of providing the contracted services;

22.3.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

22.3.3 the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place; and

22.3.4 a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained (in the case of a third party Processor) or if an information sharing protocol or agreement is in place (in the case of a third party Controller).

22.4 Please ask the DPO for assistance if you have any queries.

23 Monitoring and Review of this Data Protection Policy

23.1 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.

23.2 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.

23.3 This Data Protection Policy does not override any applicable national data privacy laws and regulations.

24 Definitions and interpretation

Automated Decision-Making (ADM) means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing;

Automated Processing means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's

performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data;

CGA means the Community Gateway Association group member which is acting as a Controller;

CGA Personnel means all employees, workers, contractors, volunteers, and trustees;

Consent means agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them;

Controller means the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to CGA's Personnel and Personal Data used in our business for our own commercial purposes;

Criminal Convictions Data means personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings;

Data Subject means a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data;

Data Privacy Impact Assessment (DPIA) means tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data;

Data Protection Officer (DPO) means the individual for responsibility for data protection compliance at CGA.

Explicit Consent means consent which requires a very clear and specific statement (that is, not just action);

Personal Data means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an

individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour;

Personal Data Breach means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach;

Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR;

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies means separate notices setting out information that may be provided to Data Subjects when CGA collects information about them. These notices may take the form of:

(a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

(b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties;

Pseudonymisation or Pseudonymised means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure;

Related Policies means CGA's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on Smartspace;

Special Categories of Personal Data means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical

or mental health conditions, sexual life, sexual orientation, biometric or genetic data; and

UK GDPR means the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Appendix 1

Vulnerability Data Policy

1 Introduction and Scope

1.1 Community Gateway Association Ltd (**CGA Ltd**) is committed to protecting the privacy and rights of our residents, particularly those who are vulnerable. This Vulnerability Data Policy is an integral part of our overarching Data Protection Policy and outlines our approach to handling Vulnerability Data in compliance with the UK GDPR and the Data Protection Act 2018.

1.2 This policy applies to all directors, employees, volunteers, contractors, and external organisations employed as processors and any external organisations or individuals with whom CGA Ltd shares or discloses Vulnerability Data. It covers all forms of data processing, including collection, storage, use, sharing, and disposal of Vulnerability Data, regardless of the medium or format

1.3 CGA Ltd collects Vulnerability Data (see paragraph 3 below for what this is) in line with its obligations set by the Regulator of Social Housing, who has set out Consumer Standards, with further guidance contained in the Consumer Standards Code of Practice. CGA Ltd has to comply with these Standards as a regulatory requirement.

1.4 This obligation is only applicable to CGA Ltd and not to any other group member. As a result, Vulnerability Data should not be shared with any other group member.

2 Policy Objectives

2.1 As a social landlord, we are committed to ensuring that our vulnerable residents can access our services and that those individuals receive the services and assistance they require from us. To achieve this, we aim to:

2.1.1 ensure that we are meeting our regulatory requirements under the Consumer Standards;

2.1.2 ensure compliance with relevant data protection legislation, including the UK GDPR and the Data Protection Act 2018;

2.1.3 use all information available to us to identify if an individual is vulnerable and to record complete and accurate details of those vulnerabilities;

2.1.4 take account of any known vulnerabilities when delivering our services and to assist vulnerable individuals in accessing our services;

2.1.5 safeguard the rights and privacy of individuals whose Vulnerability Data we process;

2.1.6 provide clear information to individuals about how their Vulnerability Data is processed;

2.1.7 establish clear responsibilities and procedures for the processing of Vulnerability Data; and

2.1.8 implement appropriate technical and organisational measures to protect Vulnerability Data from unauthorised access, loss, or damage.

3 What Is Vulnerability Data?

3.1 Vulnerability Data refers to any information related to a resident that indicates or identifies their potential or actual need for additional support or accommodations due to personal, social, economic, or health-related circumstances. This data may include, but is not limited to:

3.1.1 Health and disability information: details about physical or mental health conditions or disabilities that may affect a person's ability to live independently or access services;

3.1.2 Social and economic factors: information about financial hardship, unemployment, or other socio-economic challenges that may impact a person's housing stability or access to services, for example, if an individual is a recent care-leaver, a refugee or asylum seeker, or has recently left supported accommodation, is dealing with anti-social behaviour or has recently left a relationship which featured domestic violence;

3.1.3 Support needs: information about the need for social services, care, or support from external agencies or organisations; and

3.1.4 Communication preferences: specific requirements for communication methods or formats due to disabilities or language barriers.

4 Identifying and recording Vulnerability Data

4.1 We can identify Vulnerability Data in a number of different ways, including through:

4.1.1 information provided directly by residents when they: (i) apply for housing; (ii) contact us; or (iii) complete a survey;

4.1.2 any member of staff who has contact with vulnerable individuals, whether in person, over the phone or via other communication channels;

4.1.3 our contractors; or

4.1.4 referrals from external agencies or organisations.

4.2 We will record on our systems any identified vulnerabilities, specific communication or access needs, and whether there are any individuals with delegated authority, such as care or support workers, to communicate on behalf of the individual.

4.3 Vulnerability is a dynamic condition that can change depending upon the circumstances. As a result, we must ensure that any Vulnerability Data we hold is kept up-to-date and readily accessible so that we can ensure that we are meeting our obligations to vulnerable individuals.

5 Lawful Basis and Legal Condition for Processing Vulnerability Data

5.1 Lawful basis

5.1.1 The lawful basis we rely upon to process any personal data contained within Vulnerability Data is set out in Article 6(1)(c) of the UK GDPR which states that "processing is necessary for compliance with a legal obligation to which the controller is subject".

5.1.2 The specific legal obligations we rely upon are those set out in the Consumer Standards established by the Regulator of Social Housing pursuant to its powers under Housing and Regeneration Act 2009 and the Social Housing (Regulation) Act 2003, which require us to collect information about our residents' vulnerabilities and diverse needs.

5.2 Condition for Processing Special Category Data

5.2.1 Vulnerability Data may include special category data. Special category data is defined in Article 9(1) of the UK GDPR as "personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, 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".

5.2.2 We must always meet a condition when we deal with special category data. If data is provided to you and you do not believe that it falls within one of the two potential conditions below then please contact your Manager or our DPO for further advice.

5.2.3 The conditions we rely upon for processing special category data are either:

(a) Substantial public interest for the purpose of safeguarding vulnerable individuals in accordance with Article 9(2)(g) of the UK GDPR and condition 18 of Schedule 1 to the Data Protection Act 2018; or

(b) our legal obligation to provide housing in accordance with the Regulatory Standards and Article 9(2)(b) of the UK GDPR.

6 Data Minimisation and Retention Procedures

6.1 Data Minimisation

6.1.1 **Purpose limitation**: We will only collect and process Vulnerability Data that is directly relevant and necessary for fulfilling our legal and regulatory obligations. Data collection will be limited to what is required to achieve these purposes.

6.1.2 **Regular audits**: Regular audits will be conducted to ensure compliance with data minimisation principles. Any data deemed unnecessary will be securely deleted.

6.2 Data Retention

6.2.1 **Data Retention Schedule**: Vulnerability Data will be retained in accordance with our Data Retention Schedule.

6.2.2 **Secure disposal**: Vulnerability Data will be securely deleted or destroyed once it is no longer required for the purposes for which it was collected.

7 Data Subject Rights

7.1 Rights and Limitations

7.1.1 **Rights of Access and Rectification**: Data subjects have the right to access their data and request corrections if necessary. We will provide mechanisms for data subjects to exercise these rights efficiently.

7.1.2 **Limitations**: As we are processing Vulnerability Data on the basis of our legal obligations, residents do not have the right to erasure, data portability, or the right to object. This is to ensure that we can fulfil our regulatory obligations to the Regulator of Social Housing without interruption.

7.2 **Transparency and Communication**

7.2.1 **Transparency**: We will provide clear and concise information to individuals about the processing of their Vulnerability Data, including the legal basis, legal condition, purpose, and retention period, through our privacy notices.

7.2.2 **Communication**: We will establish dedicated communication channels for individuals to inquire about their data and exercise their rights. This includes providing a contact point for the Data Protection Officer to address inquiries and facilitate the exercise of those rights.

8 Monitoring and Review

8.1 **Annual review**: This policy will be reviewed annually or as required to ensure compliance with legal requirements and best practices. The review will take into account legislative changes, updates in regulatory guidance, and evolving operational needs.

8.2 **Stakeholder feedback**: Feedback from stakeholders, including residents, and colleagues, will be considered in the review process to ensure the policy remains effective and relevant.

9 Contact Information

9.1 For questions or concerns regarding this policy, please contact the Data Protection Officer (DPO) using the contact information set out in the Data Protection Policy.

community gateway