Calvay Housing Association Limited

DATA PROTECTION POLICY

Date Approved:	April 2018
Date Reviewed:	November 2019
Date of Next Review:	April 2021

1. INTRODUCTION

1.1 Calvay Housing Association needs to collect and use certain types of information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact in order to carry out its work. The General Data Protection Regulation 2016 (GDPR) requires organisations to meet certain obligations when processing personal information to prevent that information being improperly used or distributed. The individual (known as the data subject) whose personal data is being held also has a right to know exactly what information is being held about them and why it is held.

1.2 This policy describes how personal data must be collected, handled and stored to meet the data protection standards and to comply with the law.

2. WHY THIS POLICY EXISTS

2.1 This data protection policy ensures Calvay Housing Association:

- Complies with data protection law and follows good practice
- Protects the rights of employees, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of data breach

3. POLICY SCOPE

3.1 This policy applies to:

- Any office of Calvay Housing Association
- All employees, Committee members and volunteers of Calvay Housing Association
- All contractors, suppliers and other people working on behalf of Calvay Housing Association

4. RESPONSIBILITIES

4.1 Everyone who works for or with Calvay Housing Association has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

4.2 However, the following people have key areas of responsibility:

- The Management Committee is ultimately responsible for ensuring that Calvay Housing Association meets its legal obligations.

- The Corporate Services Manager, who for the purpose of this policy is the Data Protection Co-ordinator, is responsible for:
  - Ensuring employees and the Management Committee are regularly updated on data protection responsibilities, risks and issues

- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from employees and anyone else covered by this policy
- Dealing with requests from individuals to see any data that Calvay Housing Association holds about them (this is known as a 'subject access request')
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- Liaising with the Director, to approve any data protection statements attached to communications such as the newsletter or website
- Liaising with ICO regarding any data breaches

- The Corporate Services Manager, with the support of Clearview Networks Ltd , is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable standards
  - Performing regular checks and scans to ensure that security hardware and software is functioning properly
  - Evaluating third-party services Calvay Housing Association is considering using to store or process data.

5. GENERAL DATA PROTECTION REGULATION 2016 (GDPR)

5.1 To comply with the GDPR, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. These rules apply regardless of whether the personal data is collected on paper, stored in a computer database or recorded on other material. The GDPR covers the collection and processing of images of individuals caught by CCTV cameras. The GDPR principles apply to digital images as much as they apply to documents.

5.2 Calvay Housing Association is the Data Controller under the Regulation, which means that it determines what purposes any personal information held, will be used for. It is also responsible for notifying the Information Commissioner's Office (ICO), who is the supervisory body, of the data it holds or is likely to hold and the general purposes that this data will be used for.

5.3 To this end anyone who, on behalf of the Calvay Housing Association, processes personal information will adhere to the six principles of data protection. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

THE SIX DATA PROTECTION PRINCIPLES ARE:

1. **Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals**

   Processing shall be lawful only if at least one of the following applies:

   - Data subject has given consent
   - There is a legal obligation to process the personal data
   - Processing the data is in the public interest
   - Processing the data is necessary for the performance of contract
   - To protect vital interest
   - There is a legitimate interest

   Consent as a ground of processing will require to be used from time to time by the Association when processing personal data. It should be used where no other alternative ground for processing is available. In the event that consent is required to process a data subject's personal data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained must be for a specific and defined purpose (i.e. general consent cannot be sought).

   The Association must be fair and transparent with the data subject at the point of collecting data. This allows the data subject to make an informed decision to provide the data if they know what the organisation is going to do with it. It would not be considered fair if personal data is collected for one purpose and then used for another without the data subject being advised when it was collected that this may be the case.

2. **Data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**
   Having given notice to the individual of the purpose for which the information is to be used, it should not be used for any other purpose.

3. **Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**
   The Association and its subsidiaries will identify the minimum amount of information that is required in order to fulfil its purpose.

4. **The data shall be accurate and kept up to date**
   Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed is erased or rectified without delay.

5. **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes**
   The Association and its subsidiaries will regularly review the information kept and will delete or destroy that which is no longer required as detailed in the document retention schedule.

6. **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.**
   The Association will take reasonable steps to ensure that staff members only have access to data required for them to carry out their duties and provide them with appropriate training. Risk assessments will be carried out to identify and manage the risk of breach of security.

6. PERSONAL DATA

6.1 Personal data is any information relating to an identified or identifiable living natural person (data subject) directly or indirectly through one or more pieces of such information.

General personal data includes but is not limited to:

- First and last name
- Address
- Tenancy reference number
- Location data
- Online identifier (i.e. IP Address)
- Video/CCTV
- Bank account information
- Passport information
- Personal email address
- Credit card information
- Photos and videos
- Usernames and passwords

Special categories of personal data include:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Data concerning health
- Sex life or sexual orientation
- Criminal convictions and offences

6.2 Collecting and processing of special category (sensitive) data is prohibited unless an Article 9.2 exemption applies. The exemptions which allow organisations to process such data are:

- The data subject has given explicit consent
- The controller has a legal obligation with regard to employment, social security and social protection as set out in law by a Member State
- Such processing is necessary to protect the vital interests of the data subject
- Foundations, associations or other non-profit bodies with political, philosophical, religious or trade union aims processing such data in accordance with their

legitimate activities providing such activities apply only to members or former members with regular contact
- The data subject has made such information public
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing is in the public interest where such processing is proportional to the aim pursued
- Processing relates to occupational health to assess the working capacity of an employee, provision of treatment or management of health or social care
- Processing is necessary for public health
- Processing is for public interest, scientific or historical research purposes or for statistical purposes

7. THE RIGHTS OF INDIVIDUALS

7.1 Under the GDPR, individuals (data subjects) have a number of rights against the Association and its subsidiaries as listed below.

7.2 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data.

We must provide individuals with a 'fair processing notice' at the time of collecting their personal data from them this includes:
- Our purpose for processing their personal data
- Our retention periods for that personal data
- Who the data will be shared with

If we obtain personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no longer than one month. The privacy information that we provide must be concise, transparent, intelligible, and easily accessible and it must use clear and plain language.

We must regularly review, and where necessary update our privacy information and we must bring any new uses of an individual's personal data to their attention before we start the processing.

7.3 The right of access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR individuals have the right to obtain:
- Confirmation that their data is being processed
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in the fair processing notice

If an individual contacts the Association or one of its subsidiaries requesting this information, this is called a Subject Access Request (SAR). The SAR procedure will be followed and the Data Protection Co-ordinator will take a lead in this process.

7.4 The right to rectification

Individuals have the right to have inaccurate information rectified, or completed if it is incomplete. The request can be made verbally or in writing and we must respond to the request within one calendar month. The Data Protection Co-ordinator will deal with this request. In certain circumstances a request for rectification can be refused.

7.5 The right to erasure (the right to be forgotten)

Individuals have the right to have their personal data erased, the right to erasure is also known as 'the right to be forgotten'. The request can be made verbally or in writing and we must respond to the request within one calendar month. The right is not absolute and only applies in certain circumstances.

7.6 The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, it is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing and a response must be provided within one calendar month.

7.7 The right to data portability

The right to data portability allows individual to obtain and reuse their personal data

7.8 The right to object

Individuals have the right to object to specific types of processing:

- Direct marketing
- Processing based on legitimate interests or performance of a task in the public interest/exercise of official authority; and
- Processing for research or statistical purposes

Only the right to object to direct marketing is absolute (i.e. there is no need for the individual to demonstrate grounds for objecting, there are no exemptions which allow processing to continue). The Association and its subsidiaries is obliged to notify individuals of these rights at an early stage through the Fair Processing Notice.

7.9 Rights in relation to automated decision making and profiling

Where an individual has objected to automated decision making they have a right to request human intervention. Controllers who are direct marketing are obligated to bring the right to object and how to do that to the attention of the data subject.

8. CHILDREN

Where any personal information about children (under the age of 13) is collected consent from the parent or guardian will be obtained.

9. DATA BREACH

A breach must be reported to the ICO within 72 hours of the breach being identified even if the investigation is still ongoing. If the Association or one of its subsidiaries fail to report a breach within this timescale it must demonstrate to the ICO why it did not do so and if the ICO deem the delay unjustified, a fine may be imposed.

10. CCTV IMAGES

10.1 The right of access for individuals to information held about them and the right to stop or prevent processing likely to cause damage or distress and the right to compensation for unlawful processing all apply to CCTV images.

10.2 If the images are taken with a view to passing them on to a third party, the Association will ensure that the decision to do so is taken only by a senior member of staff who has been trained in the Data Protection principles.

11. EXEMPTIONS

11.1 The Association can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in order to safeguard:

- National security
- Defence
- Public security
- The prevention, investigation, detection or prosecution of criminal offences
- Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security
- The protection of judicial independence and proceedings
- Breaches of ethics in regulated professions
- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention
- The protection of the individual, or the rights and freedoms of others
- The enforcement of civil law matters

12. FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

12.1 The Freedom of Information (Scotland) Act 2002 applies to Housing Associations and Co-operatives in Scotland from 11 November 2019. The Association's appointed Data Protection Officer (DPO), registered with the Information Commissioner's Office, is RGDP LLP (www.rgdp.co.uk).