

# Data Protection

---

If you have difficulty with sight or hearing, or if you require a translated copy of this document, we would be pleased to provide this information in a form that suits your needs.

	<b>Policy number:</b>	<b>C8</b>
	<b>Policy approved on:</b>	May 2015
	<b>Due for review:</b>	May 2018

## **Our Vision, Mission Statement and Values**

Glen Oaks' vision statement '**Where Communities Thrive**' and our mission statement '**Our aim is to provide good quality affordable housing and an excellent service. We will encourage resident participation and work with other agencies to regenerate our community**' provide the foundation for Glen Oaks Housing Association's commitment to its residents and the communities they live in.

This commitment is also demonstrated in the Association's values which were agreed following discussions with the Board and staff. Glen Oaks' values are fundamental to how we carry out our day-to-day activities.

Our values are:

### **respectful**

*we trust and respect our customers and each other*

### **dedicated**

*we will give 100% commitment to our work*

### **transparent**

*we will be open and honest about what we do*

### **aspirational**

*we will strive to achieve the best we can for our communities*

## **Equality & Diversity Statement**

The Association is intent on ensuring people or communities do not face discrimination or social exclusion due to any of the following protected characteristics: age; disability; sex; marriage & civil partnership; race; religion or belief; sexual orientation; gender reassignment; pregnancy & maternity.

This document complies with the Association's equality & diversity policy.

The Association will regularly review this document for equal opportunities implications and take the necessary action to address any inequalities that result from the implementation of the policy.

# Contents

---

<b>Section</b>		<b>Page</b>
1.0	Introduction	1
2.0	Aims and objectives	1
3.0	General Data Protection Regulation 2016 (GDPR)	1
4.0	Responsibilities	2
5.0	Data protection principles	2 - 4
6.0	Personal data	4 - 5
7.0	Fair Processing Notice	5
8.0	Data sharing	5 - 6
9.0	The rights of individuals	6 - 7
10.0	Children	8
11.0	Data breaches	8
12.0	Physical security	8
13.0	Personal Impact Assessments	8 - 9
14.0	Exemptions	9
15.0	Freedom of Information (Scotland) Act 2002	9 - 10
16.0	Training	10
17.0	Monitoring and reviewing policy	10

## **1.0 Introduction**

1.1 Glen Oaks 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 Association 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.

## **2.0 Aims and objectives**

2.1 The Association will ensure that all personal information is dealt with properly, regardless of how it is collected, recorded and used. This policy will promote good practice and allow the Association to comply with the principles outlined in the GDPR.

2.2 This policy applies to all employees, Board members and volunteers of the Association. Contractors, suppliers and other people working on behalf of the Association will need to adhere to this policy in order to ensure the Association's compliance with GDPR.

## **3.0 General Data Protection Regulation 2016 (GDPR)**

3.1 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 data is collected on paper, stored in a computer database or recorded on other material. The GDPR principles apply to digital images as much as they apply to paper documents.

3.2 Glen Oaks Housing Association is the Data Controller under GDPR, 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) of the data it holds or is likely to hold and the general purposes that this data will be used for.

## **4.0 Responsibilities**

4.1 Everyone who works for Glen Oaks 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 the six data protection principles.

4.2 The following people have key areas of responsibility

- The Board is ultimately responsible for ensuring that the Association meets its legal obligations
- The Corporate Management Team is responsible for:
  - Checking and approving any contracts or agreements with third parties that may handle the Association's personal data
- The Finance Director / Senior IT Officer are 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 are functioning properly
- The Corporate Services Manager, who for the purpose of this policy is the Data Protection Co-ordinator, is responsible for:
  - Ensuring employees and the Board are regularly updated on data protection responsibilities, risks and issues
  - Reviewing data protection procedures and related policies
  - Arranging data protection training and advice
  - Handling data protection questions from employees and anyone else covered by this policy
  - Dealing with requests from individuals to see any data that the Association holds about them i.e. subject access requests
  - Liaising with the ICO regarding any data breaches

## **5.0 Data protection principles**

5.1 *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 the vital interest of the data subject or another person
- 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 will be obtained 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. 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 Association 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.

5.2 *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.

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

5.4 *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.

5.5 *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 will regularly review the information kept and will delete or destroy that which is no longer required as detailed in the document retention schedule.

5.6 *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.

## **6.0 Personal Data**

6.1 Personal data is that from which a living individual can be identified either by that data alone or in conjunction with other data held by the Association.

General personal data includes but is not limited to:

- First and last name
- Address
- Tenancy (or owner) reference number
- Location data
- Online identifier (i.e. IP address)
- Video / CCTV
- Bank account details
- 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

## **7.0 Fair Processing Notice**

7.1 The Association must provide a Fair Processing Notice to customers at the time of collecting their personal information.

7.2 An Employee Fair Processing Notice will be provided to all employees of the Association.

## **8.0 Data Sharing**

8.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with data protection laws, we will require the third party organisations to enter into an

agreement with the Association. This will govern the processing of data, security measures to be implemented and responsibility for breaches.

## **9.0 The rights of individuals**

9.1 Under the GDPR individuals (data subjects) have a number of rights against the Association as listed below.

### *9.2 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.

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. 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.

### *9.3 The right of access*

The right of access allows individuals to be aware of and verify the lawfulness of the processing.

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 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.

### *9.4 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 this request within one calendar month. The data

Protection Co-ordinator will deal with these requests. In certain circumstances a request for rectification can be refused.

9.5 *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 request is not absolute and only applies in certain circumstances.

9.6 *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.

9.7 *The right to data portability*

Individuals have the right to obtain and reuse their personal data.

9.8 *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 is obliged to notify individuals of these rights at an early stage through the Fair Processing Notice.

9.9 *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 must bring to the attention of the data subject the fact that they have the right to object and explain how to do that.

## **10.0 Children**

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

## **11.0 Data breaches**

A breach must be reported to the ICO within 72 hours of it being identified even if the investigation is still ongoing. If the Association fails to report a breach within this timescale, it must demonstrate to the ICO why this happened and, if the ICO deem the delay unjustified, a fine may be imposed.

## **12.0 Physical security**

12.1 The Association will take appropriate physical security measures to prevent unauthorised access to, or loss, alteration or damage of personal data.

12.2 Physical security measures will include:

- The office will be kept secure, within and outwith working hours so that unauthorised persons cannot access the Association's personal data records.
- When personal data is no longer required it must be disposed of securely by the employee responsible for it
- Employees will log out of the network or lock their computer screen when leaving their desks
- Computer terminals which are not in use will be logged off the network by the last user before leaving the terminal
- No personal data will be stored in areas of the office where unauthorised persons have unsupervised access.
- Contractors and other third parties will agree to comply with GDPR as a condition of their contract.

## **13.0 Personal Impact Assessments**

- 13.1 Personal Impact Assessments (PIAs) will be used to help the Association identify and reduce the risks that our operations have on personal privacy of data subjects.
- 13.2 The Association will carry out a PIA before undertaking a project of processing activity which poses a “high risk” to an individual’s privacy. High risk can include (but is not limited to) activities using information relating to health or race, or the implementation of a new IT system for storing and accessing personal data.
- 13.2 The PIA should include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures the Association will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

## **14.0 Exemptions**

- 14.1 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

## **15.0 Freedom of Information (Scotland) Act 2002**

15.1 The Freedom of Information (Scotland) Act 2002 does not currently apply to housing associations in Scotland. However, the Association has adopted the principle of being as open as possible in its business, and restricting the withholding of information solely to that of commercially sensitive information.

## **16.0 Training**

16.1 The Association will provide appropriate training to all employees who record personal information.

## **17.0 Monitoring & reviewing policy**

17.1 We will review the policy every three years. More regular reviews will be considered where, for example, there is a need to respond to new legislation / policy guidance.