# Yorkhill Housing Association Limited

# Data Protection Policy
# May 2018

## Contents

## 1. Purpose of Policy

Yorkhill Housing Association needs information to carry out its business and provide services to its tenants and factored property owners.

We will make sure that any personal information we have to allow us to do this is kept safe and in line with the law. We will always do this in the best way we can.

We set out here how we will do this.

## 2. The Association's Legal Responsibility

We will collect, hold and use personal information in ways that meet with the law.

**Law on information**

(a) the General Data Protection Regulation (E.U.) 2016/679 (the G.D.P.R.);

(b) the Privacy and Electronic Communications (E.C. Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(c) any law that the United Kingdom puts in place, the General Data Protection Regulation (E.U.) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and if the United Kingdom leaves the European Union.

This policy complies with our legal requirements.

## 3. Data

3.1 We hold a variety of information on people like customers and staff (data subjects) which is known as Personal Data. The Personal Data held and processed by us is noted in our Privacy Notices that are given to all our customers including tenants, factored property owners, job applicants, employees, housing applicants and members.

3.1.1 'Personal Data' is information that can identify someone on its own or along with other information.

3.1.2 We also hold sensitive information like racial or ethnic origin, religious beliefs, political opinions, health or sexual orientation. This is 'Special Category Personal Data' or 'Sensitive Personal Data'.

## 4. Processing of Personal Data ('processing' means anything or set of things which is undertaken with personal data')

**4.1** We are permitted to process Personal Data if:

- you say we can;
- it is needed for a contract with you;
- to meet the law;
- to protect your own or someone else's vital interests;
- it is in the public interest; and
- it is necessary for interest allowed by the law.

### 4.2 Privacy Notices

4.2.1 We have Privacy Notices we must give you which explains our use of your information. We will give these to you at the start of our business together.

### 4.3 Employees

4.3.1 Employee data is held and processed in line with this policy. What, why and how is stated in the Employee Privacy Notice that staff receive with their contract of employment. All information held can be obtained from the Chief Executive on request.

### 4.4 Consent

If we need your agreement to use information of yours we will give you a form to sign. The form will let you know what we will use the information for.

### 4.5 Processing of Special Category Personal Data or Sensitive Personal Data

If we are using your information it will only be if:

- you agree; or
- it's for employment or social security reasons; or

- we need it to protect your own or someone else's vital interests;
- it is needed to meet the law; or
- it is of significant public interest.

## 5. Data Sharing

5.1 If we share information with others we will agree how we will use it, keep it safe and in a way that meets with the law. 'Data Sharing Agreement'.

5.1.1 Where we and others require to use the same personal information we will both be data controllers.

### 5.2 Data Processors

5.2.1 A data processor is someone that processes information for us. They must comply with the law and show us they can do this.

5.2.2 If they breach the law in any way they must let us know.

5.2.3 If a data processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for data protection breaches of their sub-contractors.

5.2.4 If we contract a third party to process personal data held by us we will enter into a Data Processing agreement.

## 6. Data Storage and Security

All Personal Data held by us will be stored securely, whether electronically or on paper.

### 6.1 Paper Storage

All personal information will kept out of site, locked away when not being used and will only be available to authorised people.

### 6.2 Electronic Storage

Personal Data stored electronically will also be protected from unauthorised use and access. Personal Data will be password protected when being sent internally or externally to the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal data is stored on removable

media (C.D., D.V.D., U.S.B. memory stick) then that removable media will be stored securely at all times when not being used. Personal Data will not be saved directly to mobile devices and will be stored on designated drivers and servers.

## 7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported.

### 7.2 Internal Reporting

We take the security of data very seriously.

- If a breach or potential breach has occurred, our Compliance Manager will be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- We will seek to contain the breach by whatever means available;
- We will consider whether the breach is one which requires to be reported to the Information Commissioners Office (I.C.O.) and data subjects affected.
- We will notify third parties in line with the terms of any Data Sharing and Data Processing agreements.

### 7.3 Reporting to the I.C.O.

We will report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of a breach to the Information Commissioner's Office.

## 8. Named Officer

Our Compliance Manager is the named officer and will be responsible for:

8.1.1 Monitoring the Association's compliance with Data Protection laws and this Policy.

## 9. Data Subject Rights

9.1 You are entitled to view personal information we have on you.

9.2 You have the right to limit information we hold on you, and to be forgotten. Our Privacy notices explain these rights.

9.3 **Subject Access Requests**

You can view the information we have on you by making a ‘Subject Access Request’.

If you do this we will answer you within one month of receiving your request. We will:

9.3.1 Provide you with an electronic or hard copy of your information, unless the law provides otherwise.

9.3.2 Where information relates to others we will seek their permission before releasing it.

9.3.3 If we don’t have the information you are asking for we will let you know within one month from when you ask for it.

9.4 **The Right to be Forgotten**

9.4.1 If you wish you can write to us and ask us to remove all information we have on you.

9.4.2 If you do we will consider how and what we can remove but always in terms of law.

9.4.2 We will let you know what we have removed or what we have to keep and why.

9.5 **The Right to Restrict or Object to Processing**

9.5.1 You may object to or ask us to limit the information we process.

9.5.1.1 We will not use your information for marketing.

9.5.2 Any restriction request or objection received will be passed to the Compliance Manager. Legal advice may be sought by the Association and will be followed.

## 10. Privacy Impact Assessments (P.I.A.s)

a. These will help us identify and reduce any risk regarding information use.

b. We will:

i. Carry out a P.I.A. if we are doing any system or policy change.

ii. In doing this we will carry out a risk assessment.

10.1 If any high risks are identified and cannot be reduced the I.C.O. will be told.

## 11. Archiving, Retention and Destruction of Personal Data

We will make sure that all personal data is held only for the periods noted below and then archived or destroyed securely.

| Subject | Type of Information | Retention Period |
|---|---|---|
| **Employees** | **Paper Copies:** Personal information. | Will be retained securely for 5 years after an employee leaves the Association. After 5 years the employees name, position and length of service only will be kept in the archive register of former employees. . All other information will be destroyed in accordance with the Association's secure disposal processes. |
| | **Electronic:** All information held electronically will be permanently deleted from the Association's system. | Permanently deleted on subject leaving the organization. |

| | | |
|---|---|---|
| **Factoring** | **Paper and electronic:** Minutes of Factoring Meetings. | Duration of Association's appointment as Factor. |
| | General Correspondence. | 5 years after sale of property. |
| | Equality and Diversity Information. | Duration of ownership. |
| | Anti-social behavior information. | Duration of ownership. |
| | Factoring agreements. | 5 years after sale of property. |
| | Financial Records. | 7 years. |
| **Housing Management** | Paper records. | Personal information 5 years after your tenancy ends. |
| | Electronic Records. | Securely archived and only accessed by relevant staff. |
| | Paper housing applications. | For as long as your stay on our housing waiting list. |
| | Electronic housing applications. | Securely archived and only accessed by relevant staff. |
| **Maintenance** | Electronic only. | Held on Association database only for duration of tenancy. |

When retention periods are ended all information will be destroyed in accordance with the Association's secure disposal processes.

**Related Documents**

- General Privacy Notice
- Factoring Privacy Notice
- Employee Privacy Notice
- Committee Members Privacy Notice
- Association Members Privacy Notice
- Contractors Addendum
- Data Sharing Agreement
- Subject Access Request