PRIVACY POLICY

Classification: Management

Status: Approved

Policy Lead:	Chief Executive Officer
Date Approved:	May 2018
Last Review Date:	May 2018
Review Due Date:	May 2021
Review Period:	3 years

REFERENCE PAGE

Document Title:	Privacy Policy
Aim:	
Objective:	**Strategic Objective 01 - Governance**
Strategy Reference:	
Customer Service Standards Reference:	
Scope of Policy:	
Responsible Officer:	
Dates of Adoption / Review:	May 2018
Approval Source:	Executive Team
Legal and Regulatory References:	**The relevant legislation in relation to the processing of data is :** • the General Data Protection Regulation (EU) 2016/679 ("the GDPR"); • The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and • any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union
Procedural References:	
Consultation Completed:	
Risk Implications:	
Equalities Assessment:	
Monitoring Arrangements / Requirements:	
Accessibility:	
Supporting Documents:	• Customer Fair Processing Notice • Employee Fair Processing Notice • Contract Clause for Employees • Data Sharing Agreement • Data Sharing Addendum • Sharing Personal Data (Guidance) • Access to Personal Data (Procedure)

Contents

1. Introduction

Eildon Housing Association (hereinafter “Eildon”) is committed to ensuring the secure and safe management of data held by Eildon in relation to customers, staff and other individuals, also referred to as Data Subjects. Eildon’s staff members have a responsibility to ensure compliance with the terms of this policy and to manage individuals’ data in accordance with the procedures created to accompany this policy.

Eildon needs to gather and process information about individuals, including personal and sensitive category information. These individuals may be customers, see glossary, employees and other individuals with whom Eildon have a relationship with.

This policy defines the parameters for management of personal data and Eildon’s duties in the processing of that data. See reference page for supporting documentation.

2. Data

2.1 Customer Data

The data that Eildon holds and processes about customers is detailed within the Customer Fair Processing Notice (FPN), see supporting documents. The Customer FPN sets out the Personal Data processed by Eildon and the basis for processing that data. The Customer’s FPN is provided to all Eildon customers at the outset of processing their data.

The Customer FPN gives customers information on how to request a copy of their personal information that Eildon processes.

2.2 Employee Data

The Employees FPN details the data held and processed about Eildon employees, this is provided to all employees at the same time as their contract of employment. A Contract Clause of Terms and Conditions of Employment in regard to Data Protection has been issued to all staff members employed prior to 25 May 2018.

A copy of any employee’s Personal Data held by Eildon is available upon written request to the Data & Information Officer.

3. Processing of Personal Data

Eildon is permitted to process personal data on behalf of Data Subjects provided it is doing so on one of the following grounds:

- with the consent of the data subject (see clause 3.1 hereof);
- is necessary for the performance of a contract between Eildon and the data subject or for entering into a contract with the data subject;
- is necessary for Eildon's compliance with a legal obligation;
- is necessary to protect the vital interests of the data subject or another person;
- is necessary for the performance of a task carried out in the public interest or in the exercise of Eildon's official authority; or
- is necessary for the purposes of legitimate interests.

3.1 Consent

Consent as a ground for processing will be used from time to time by Eildon when processing Personal Data. It will be used by Eildon where no other alternative ground for processing is available. In the event that Eildon requires to obtain consent to process a data subject's Personal Data, consent 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 if willing to consent. Any consent to be obtained by Eildon must be for a specific and defined purpose (i.e. general consent cannot be sought).

3.2 Processing of Special Category Personal Data or Sensitive Personal Data

If Eildon processes Special Category Personal Data or Sensitive Personal Data, this will be done in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

4. Data Sharing

Eildon shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with relevant policies and procedures. In order that Eildon can monitor compliance by these third parties with Data Protection laws, Eildon requires third-party organisations to enter in to an agreement with Eildon governing the processing of data, security measures to be implemented and responsibility for breaches.

4.1 Data Controllers

Personal data is from time to time shared between Eildon and third parties who require to process personal data that Eildon processes as well. Both Eildon and the third party will be processing that data in their individual capacities as data controllers.

Where Eildon shares in the processing of personal data with a third-party organisation (e.g. for processing of the employees' pension), it shall require the third-party organisation to enter in to a Data Sharing Agreement with Eildon in accordance with the terms of the model Data Sharing Agreement, see supporting documents.

4.2 Data Processors

Data processors are frequently engaged for certain aspects of Eildon's outsourced work (e.g. maintenance and repair work).

A data processor must comply with Data Protection laws. Eildon's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify Eildon if a data breach is suffered.

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

Where Eildon contracts with a third party to process personal data held by Eildon, it shall require the third party to enter in to a Data Protection Addendum with Eildon in accordance with the terms of the model Data Protection Addendum – see supporting documents.

5. Data Storage and Security

All Personal Data held by Eildon is stored securely, whether electronically or in paper format. See attached staff guidance for securing personal data.

6. Breaches

A data breach can occur at any point when handling Personal Data and Eildon has 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 externally in accordance with Clause 6.3 hereof.

6.1 Internal Reporting

Eildon takes the security of data very seriously and in the unlikely event of a breach has specific guidelines for staff to implement to contain, manage and report the breach.

6.2 Reporting to the ICO

The DIO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DIO will also consider whether it is appropriate to notify those data subjects affected by the breach.

7. Data & Information Officer ("DIO")

Eildon have appointed a Data & Information Officer who has an over-arching responsibility and oversight over compliance by Eildon with Data Protection laws, contact details for the DIO can be found in the FPN.

8. Data Subject Rights

Certain rights are provided to Data Subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by Eildon, whether in written or electronic format.

Data Subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to Eildon's processing of their data. These rights are notified to Eildon's customers and tenants in the Fair Processing notices.

8.1 Subject Access Requests

Data Subjects are permitted to view their data held by Eildon upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, Eildon will respond to the Subject Access Request within one calendar month of the date of receipt of the request. Eildon:

- Will provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

- Where the personal data comprises, data relating to other data subjects, will take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or:

- Where Eildon does not hold the personal data sought by the data subject, will confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one calendar month from the data on which the request was made.

See the Access to Personal Data Procedure for further guidance.

8.2 The Right to be Forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to Eildon seeking that Eildon erase the dat subject's personal data in its entirety.

Each request received by Eildon will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DIO will have responsibility for accepting or refusing the data subjects request in accordance with clause 8.4 and will respond in writing to the request.

8.3 The Right to Restrict or Object to Processing

A data subject may request that Eildon restrict its processing of the data subjects Personal Data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by Eildon a data subject has an absolute right to object to processing of this nature by Eildon, and if Eildon receives a written request to cease processing for this purpose, them it must so immediately.

Each request received by Eildon will require to be considered on its own merits and legal advice will be required to be obtained in relation to such requests from time to time. The DIO has responsibility for accepting or refusing the data subjects request in accordance with clause 8.5 and will response in writing to the request.

9. Privacy Impact Assessments ("PIAs")

PIA's are a means of assisting Eildon in identifying and reducing the risks that our operations have on personal privacy of data subjects. Eildon will:

- Carry out a PIA before undertaking a project or 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; and

- In carrying out a PIA, 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 that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

Employees are required to notify the DIO when undertaking projects that require for personal information to be shared out with the organisation.

Eildon will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The DIO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

10. Archiving, Retention and Destruction of Data

Eildon will not store and retain Personal Data indefinitely. Eildon ensures that Personal data is only retained for the period necessary, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

Eildon shall ensure that all Personal data is archived and destroyed in accordance with the retention schedule on Eildon's website, alternatively contact Eildon and ask for a hard copy of the retention schedule.

11. Complaining

Anyone unhappy with the way Eildon have dealt with their personal information should, in the first instance complain directly to the Data & Information Officer to allow the opportunity to put the situation right. For full details of the ways in which you can complain, please see our complaints procedure.

If, having followed our complaints process, you remain unhappy then you should contact the Information Commissioner's Officer. Full details are available on their website www.ico.gov.uk or you can phone them on 0303 123 1113.

12. Training

Eildon provide training to all staff and Board members to make sure that all policies work effectively.

13. Review of Policy

The Corporate Services Coordinator will ensure this policy is reviewed every 3 years or earlier if there are any change to legislation. The Executive Team have delegate authority to approve and review this management.

14. Definitions

Customer: anyone that Eildon processes personal data about, excluding employees. Including, but not limited to: tenants, factored properties, Border Care & Repair clients, Shared Owners, Mid Market Rent Tenancies, Complainants, Outreach clients, Applicants.

Data Controller: a person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.

Data Processor: In relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the data controller.

Data and Information Officer: someone to take responsibility for data protection compliance.

Data Subject: a living individual who is the subject of personal data e.g. tenant, employee, board member, suppliers.

Information Commissioners Officer (ICO): Responsible for enforcing the Regulations.

Personal Data: Personal data is defined as, data relating to a living individual who can be identified from:

A) From those data;
B) From those data and other information which is in the procession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing: in relation to information or data means obtaining, recording or holding the information or data or carrying out any operations or set of operations on the information or data.

Special Category Personal Data or Sensitive Personal Data: Personal data consisting of information as to:

- Racial, ethnic origin of the data subject
- Political opinions
- Religious beliefs, or other similar beliefs
- Member of a trade union
- Physical / mental health or conditions
- Sexual life
- Commission or alleged commission by the data subject of any offence
- Any proceedings for any offence committed or alleged to have been committed, disposal of proceedings, or sentence of any court in such proceedings.