Eastlight Community Homes

DATA PROTECTION POLICY

Contents

1. Policy Statement

1.1 Eastlight Community Homes ("Eastlight") collects and processes personal and sensitive data from our residents, employees and other stakeholders.

1.2 We have a legal duty and obligation to treat the data we collect with care and in line with the rights of Data Subjects, and all those who use our services have a right to expect that their data will be used fairly and lawfully. Data Subjects are defined as: *'the identified or identifiable living individuals to whom personal data relates.'*

1.3 This Data Protection Policy ensures that we comply with all relevant data protection legislation, and we apply the principles of data protection to all our processing, including our responsibilities to:

- process personal data fairly, transparently and for specific lawful purposes
- collect only the minimum personal data we require
- ensure that the personal data we process is accurate and up to date
- keep personal data only for as long as necessary
- ensure that personal data is held securely and protected from unauthorised and unlawful processing
- maintain up to date records of our compliance.

1.4 We will maintain a Data Protection Framework which sets out how we implement sufficient management controls to ensure legal compliance and review these documents periodically to test our compliance and meet changing legal standards.

1.5 We will ensure that all who are responsible for processing data on our behalf have received appropriate and sufficient training to do so.

1.6 The Senior Leadership Team will ensure that sufficient and appropriate resources are available to meet its own standard and legal duties.

1.7 We will uphold the rights and freedoms of our residents, partners and stakeholders, and we will ensure that those rights and freedoms are appropriately considered in the decisions we take which may affect them and support them in exercising their rights, where needed.

2. Scope

2.1 This Policy applies to all personal and special category personal data processed (see Section 5 for the definition of special category data) by Eastlight in any format, either in the role of Data Controller or a Data Processor.

- Note: A Data Controller *determines the purposes and means of the processing of personal data.* A Data Processor *engages in personal data processing on behalf of the Controller.*

2.2 This Policy is applicable to all Eastlight's Board and Committee Members, employees (permanent and temporary), volunteers, partners and any third parties who have access to the personal data Eastlight processes, or systems which process personal data.

3. Statutory Requirements

3.1 This Policy is designed to ensure Eastlight meets its legal, statutory requirements including:

- UK Data Protection Legislation
- Retained General Data Protection Regulation (EU) 2016/679 (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Privacy & Electronic Communications Regulations 2003 (PECR).

4. Roles & Responsibilities

4.1 All Eastlight staff have responsibilities in relation to this Policy, and certain roles have additional responsibility, as follows:

4.2 Chief Executive

4.2.1 The Chief Executive is the accountable officer who is responsible for the management of the organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and maintaining confidentiality is pivotal to the organisation being able to operate. Responsibilities include reporting to bodies including the ICO, RSH and others as deemed appropriate for the incident and impact.

4.3 Data Protection Manager

4.3.1 The Data Protection Manager is responsible for monitoring and ensuring compliance with this Policy and overseeing the lawful processing of all personal and special category data processed by Eastlight.

4.3.2 It is the Data Protection Manager's responsibility to fulfil their tasks as set out in UK GDPR Article 39, that is:

- to inform and advise Eastlight and its employees of their data protection responsibilities as a Data Controller and Data Processor of personal data
- to monitor compliance with data protection legislation and this Policy
- to provide advice on Data Protection Impact Assessments (DPIAs)
- to co-operate with and act as the contact point for the UK's supervisory authority – Information Commissioner's Office (ICO)
- to be the contact point for Data Subjects regarding all issues related to the processing of the Data Subjects data.

4.3.3 The Data Protection Manager can be contacted at DPA-FOI@eastlighthomes.co.uk.

4.3.4 The Data Protection Manager is also responsible for seeking guidance from the Technology Director where data security concerns arise.

4.3.5 They will provide advice and guidance to the organisation regarding the lawful and appropriate processing of personal and special category data.

4.4 Technology Director

4.4.1 The Technology Director shall provide technical support and guidance regarding the secure and confidential processing of personal and special category data within Eastlight, and they are responsible for addressing any data security concerns.

4.4.2 The Technology Director is responsible for the IT Security Policy and for reporting relevant information to the Senior Leadership Team.

4.4.3 The Technology Director will ensure that any information security incidents are appropriately managed, and they will support the Data Protection Manager with information security matters, as required.

4.5 Process Owners

4.5.1 Data processing activities are managed by nominated job roles or individuals.

4.5.2 The Senior Leadership Team shall ensure that a Process Owner is assigned to each data processing activity or operation. The Process Owner has primary operational responsibility for compliance with data protection legislation and good practice in respect of their assigned processing activities.

4.5.3 Process Owners are responsible for understanding what personal data is used in their business area and how it is used, who has access to it and why. As a result, they can understand and address risks to the data and the organisation.

4.5.4 The Data Protection Manager shall maintain a list of Process Owners and the data processing activities for which they are responsible.

4.5.5 Process Owners may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other HR/People policies, and ensuring that all staff are appropriately trained.

4.6 Board, Committee Members, Employees, Volunteers, Casual/Temporary Workers

4.6.1 Anyone who is directly engaged by Eastlight, including but not limited to Board and Committee Members, employees, volunteers and casual/temporary workers, must adhere to this Policy and all associated procedures.

4.6.2 Employees must only process personal data as authorised and necessary for the completion of their duties.

4.6.3 All processing must be carried out in accordance with data protection legislation, this Policy and associated procedures.

4.6.4 Employees must never process personal data of identifiable individuals unless the processing is part of their work, or they have been specifically authorised by the Data Protection Manager to do so.

4.6.5 Employees shall report any actual or suspected non-compliance or concerns regarding the processing of personal and special category data to the Data Protection Manager without delay.

4.6.6 Employees must attend data protection and data security training as required.

4.6.7 Employees must report all actual and suspected personal data breaches in accordance with our Data Breach Reporting Procedure. Everyone within the organisation has a duty to respect the Data Subjects' rights to confidentiality.

4.6.8 Disciplinary action and/or penalties could be imposed on employees for non-compliance with relevant policies and legislation.

5. Practice & Principles

5.1 Special Category Data/Criminal Conviction & Offence Data

5.1.1 Special categories of personal data are *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership*.

5.1.2 It also includes the *processing of genetic data (biometric data for the purpose of uniquely identifying a natural person), data concerning health or data concerning a person's sex life or sexual orientation.*

5.1.3 Eastlight will not process special categories of personal data unless it is necessary. Where it is necessary, the Data Protection Manager will ensure that the lawful grounds for such processing are documented, and they will maintain a periodic review of the necessity to process special categories of personal data.

5.1.4 If we process personal data relating to criminal convictions and offences, we will implement suitable measures, including a policy document that satisfies the requirements of the Data Protection Act 2018, Schedule 1: Parts 3 and 4.

5.2 Principles

5.2.1 Eastlight will ensure any processing of personal data is carried out in compliance with Data Protection Principles as detailed below.

5.2.2 Fairness – We will ensure personal data is processed fairly and in compliance with legislation at all times.

5.2.3 Lawfulness – We will ensure there is a lawful basis to facilitate the processing of personal data and special category data.

Where the lawful grounds are legitimate interests, a Legitimate Interests Assessment (LIA) will be undertaken and documented by the relevant employee.

Where the lawful basis is consent or explicit consent, we will ensure consent is valid and that the Data Subject is able to withdraw their consent should they choose to.

Consent shall not be valid unless:

- there is a genuine choice of whether or not to consent
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the Data Subject's wishes that signifies agreement to the processing of personal data relating to them
- the consent was given through a statement made by the Data Subject or by a clear affirmative action undertaken by them
- we can demonstrate that the Data Subject has been fully informed about the data processing to which they have consented, and we are able to prove that we have obtained valid consent lawfully
- a mechanism is provided to Data Subjects to enable them to withdraw consent as easily as it was to give, and that the Data Subject has been informed about how to exercise their right to withdraw consent.

We recognise that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between Data Controller and Data Subject. We recognise that consent cannot be considered to be forever, and we will determine a consent refresh period for every instance where consent is the lawful condition for processing.

Where consent is the lawful basis for processing, the Data Protection Manager shall ensure that consent is properly obtained in accordance with the conditions above.

5.2.4 Transparency – We will ensure that transparency is engrained in the processing undertaken by being clear, open and honest with Data Subjects. Before any processing of personal data begins, the privacy information which is provided through Privacy Notices to Data Subjects will be considered and updated where necessary to ensure it accurately reflects the processing being undertaken.

5.2.5 Purpose Limitation – We will ensure personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.2.6 Data Minimisation – We will ensure personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. We will strive to use a minimum of personal data in our data processing activities and will periodically review the relevance of the information that we collect.

5.2.7 Accuracy – We will use reasonable endeavours to maintain data as accurate and up to date as possible, in particular, data which would have a detrimental impact on Data Subjects if it were inaccurate or out-of-date.

5.2.8 Storage Limitation – We ensure that we do not retain personal data for any longer than is necessary for the purposes for which it was collected, and we will apply measures at the end of data's useful life, such as erasure or anonymisation.

5.2.9 Security – We will ensure that any personal data that we process, or others processing on our behalf, is done so in a manner that ensures security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In particular, an IT Security Policy will be maintained to ensure the confidentiality, availability and integrity of personal data.

5.2.10 Accountability – The Data Controller is responsible for overall compliance. This means that they must demonstrate that the principles outlined above are met for all personal data for which it is responsible.

The Senior Leadership Team will implement sufficient controls to ensure that Eastlight is able to demonstrate compliance with the statutory requirements, including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

5.3 Rights

5.3.1 Eastlight will ensure that any processing undertaken does not infringe people's rights, and we ensure that we have appropriate procedures in place to ensure that we can effectively manage any individual rights requests we may receive.

5.3.2 We will take appropriate steps to advise individuals of their rights and to ensure that employees are able to recognise information rights requests and handle them appropriately when received.

5.3.3 These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right to erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right to complain about our processing of personal data and the right to a judicial remedy and compensation.

5.3.4 The Data Protection Manager shall maintain a procedure setting out how information rights requests are to be handled and ensure that all relevant people are made aware of this information.

5.4 Personal Data Breaches

5.4.1 Eastlight will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this Data Protection Policy.

5.4.2 All employees and individuals with access to personal data for which Eastlight is either the Data Controller or Data Processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach (whether this is actual or suspected).

5.4.3 We will log all personal data breaches and will investigate each incident immediately.

5.4.4 Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach.

5.4.5 Data protection 'near misses' will also be recorded and investigated in the same manner as data protection breaches.

5.4.6 The Data Breach Reporting Procedure sets out responsibilities, decision-making criteria and timescales for notifying Data Subjects, and where relevant the Information Commissioner's Office (ICO), the Audit & Risk Committee and the Board.

5.4.7 The Data Protection Manager shall be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

5.4.8 The Data Protection Manager shall be responsible for ensuring that individuals accountable for reoccurring breaches undertake additional data protection training and implementing controls to alleviate the risk of another breach occurring. Where necessary, disciplinary action may be taken.

5.5 Data Sharing & Data Processors

5.5.1 Eastlight will only share personal data where we have a lawful basis, and where it is necessary to do so. Where we share data with third parties/processors, we will carry out appropriate due diligence and ensure there is an adequate Data Sharing Agreement/Data Processing Agreement in place prior to any sharing.

5.5.2 The Data Protection Manager will maintain a record of all third parties with whom data is shared and all Data Processors, and they are responsible for ensuring that appropriate agreements are in place.

5.5.3 The Data Protection Manager is responsible for maintaining the Data Sharing Procedure and the Selecting, Appointing, Managing & Decommissioning Data Processors Procedure, ensuring that all relevant people are made aware of them.

5.6 Restricted Transfers

5.6.1 Eastlight will only transfer data outside of the UK where it is strictly necessary to do so. Prior to transferring any personal data outside of the UK, referred to as 'a restricted transfer,' we will take steps to ensure there are appropriate data transfer mechanisms in place to safeguard the data.

5.6.2 The Data Protection Manager shall be responsible for maintaining the Restricted Transfer Procedure and for ensuring that all relevant people are made aware of it.

5.7 Children's Data

5.7.1 Special measures will be taken by Eastlight upon processing personal data relating to children under the age of 13, including the nature of privacy information provided and approach to information rights requests.

5.8 Data Protection Impact Assessments

5.8.1 Eastlight will adopt a risk-based approach to processing personal data, ensuring that we assess any risks to privacy or people's rights and freedoms before commencing, commissioning or changing data processing activities.

5.8.2 Where necessary, we will, as a minimum, ensure that a DPIA is undertaken where required by data protection legislation and/or when one is deemed to be desirable by the Data Protection Manager.

5.8.3 The Data Protection Manager is responsible for maintaining the DPIA Procedure and for ensuring that all relevant people are made aware of it.

5.9 Electronic Marketing

5.9.1 Eastlight is subject to certain obligations under PECR when sending marketing activities to its residents. We will ensure that appropriate consents are recorded prior to the sending of marketing materials, unless the "soft opt in" is applied.

5.9.2 The limited exception for existing residents, known as "soft opt in", allows us to send marketing texts or emails if we have obtained contact details in the course of a sale to that person, or if we are marketing similar services, and we gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

5.9.3 We will explicitly offer the right to object to direct marketing to the Data Subject at all stages of communication and in an intelligible manner so that it is clearly distinguishable from other information.

5.9.4 The Data Subject's objection to direct marketing shall be promptly honoured.

5.9.5 If a Data Subject opts out at any time, their details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

5.10 Privacy by Design and by Default

5.10.1 The UK GDPR requires Eastlight to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is called 'data protection by design and by default' and is essentially a risk-based approach incorporating a large focus on Eastlight's accountability as an employer and housing provider.

5.10.2 Eastlight will consider privacy by design and by default when processing personal and special category data. Privacy by design and by default is a legal obligation.

5.10.3 Privacy by design and by default requires us to consider data protection issues at the design stage of the processing and throughout its cycle.

5.11 Training & Awareness

5.11.1 Eastlight will ensure that all employees are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities.

5.11.2 We will also undertake data protection awareness-raising activities from time to time to keep data protection at the forefront of employees' minds. All training and awareness-raising activities will be logged.

5.11.3 Refresher training will be provided periodically.

Eastlight Community Homes
Eastlight House, Charter Way
Braintree
Essex
CM77 8FG

0330 128 0330
www.eastlighthomes.co.uk customer.services@eastlighthomes.co.uk

eastlighthomes
eastlighthomes
@eastlighthomes
eastlight-community-homes-