# Data Protection Policy

| | |
|---|---|
| **Reference** | TBC |
| **Purpose** | The purpose of this policy is to ensure that Eastlight Community Homes meets its legal, statutory and regulatory requirements under data protection laws and to ensure that all personal and special category information is processed compliantly and respects the rights of individuals. |
| **Owner** | Director of Governance |
| **Related documents** | Eastlight privacy policy<br>ICT Security Policy<br>Acceptable Use ICT Policy |
| **Approved by** | Shadow Board |
| **Date approved** | June 2020 |
| **Resident involvement** | N/A |
| **Performance Monitoring** | As legislation changes |
| **Review frequency** | To be reviewed annually |
| **Last review** | May 2020 |
| **Next review** | July 2021 |
| **Version** | V1.1 |
| **Author** | GDPR Information and Governance Manager |

# Contents

## 1. POLICY STATEMENT

1.1. Eastlight Community Homes Limited (hereafter 'Eastlight') collects and processes personal and sensitive data from our residents, employees and other stakeholders. As such we have a duty of care and an obligation under the law to treat the data we collect with care and in line with the rights of those data subjects.

1.2. This policy should be read in conjunction with the ICT Security policy which covers the technical aspects of ICT Security, the Acceptable Use ICT Policy which covers the obligations and requirements placed on the ICT service user and Eastlight's Privacy Policy which is available through our website.

## 2. SCOPE

2.1. See Appendix E for definitions.

2.2. This policy covers personal data as under General Data Protection Regulations (GDPR)

## 3. PRINCIPLES

3.1. Eastlight will adhere to all relevant current Data Protection legislation.

3.2. Eastlight will create and maintain suitable policies and procedures to ensure compliance.

3.3. Eastlight will ensure that all employees receive appropriate Information Security and Data Protection training. Training will be refreshed on an annual basis.

3.4. Eastlight will pursue a single view of the asset and a single view of the customer, one central repository of each, minimising the use of spreadsheets and alternative data sources, minimising or eliminating rekeying of data by establishing automated interfaces between internal systems and those maintained by external service providers.

3.5. Eastlight will ensure that information is stored, processed and maintained in a secure manner in line with current best practice.

3.6. Eastlight will take active steps to highlight our residents', service users' and stakeholders' rights under the legislation.

3.7. Eastlight will maintain a Publication Scheme and respond to reasonable requests for information about the organisation in a manner consistent with its legal requirements.

## 4. AIMS AND OUTCOMES

### 4.1. INTRODUCTION

4.1.1. The aim of this policy is to ensure that Eastlight meets its legal, statutory and regulatory requirements under data protection laws and to ensure that all personal and special category information is processed compliantly, and in the individuals' best interest.

4.1.2. The data protection laws include provisions that promote accountability and governance therefore Eastlight has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal

data.

4.1.3. This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

4.1.4. This policy applies to employees, involved residents, consultants, Board members, volunteers, representatives of Eastlight and contractors (third parties) engaged to carry out duties and manage Eastlight data on our behalf and by our instructions.

4.1.5. Complaints relating to alleged breaches of the General Data Protection Regulations will be managed through our Complaints Policy.

4.1.6. Any breaches in policy must be reported to the Governance team for evaluation and response.

4.1.7. The responsibility for data protection is outlined below:

| | |
|---|---|
| Overall responsibility | Board |
| Monitoring responsibility | Audit & Risk Committee |
| Executive lead | Executive Director Resources |
| Leadership Team lead | Director of Governance |
| Management lead | GDPR Information and Governance Manager |
| Operational | All employees (Service Users) |

## 4.2. **DATA PROCESSING**

4.2.1. Eastlight will only process personal data that has been obtained fairly and lawfully and for a specific set of purposes. Data collected will be adequate and relevant for those purposes, maintained accurately and not retained for any longer than is necessary. See Appendix D for legal bases for processing.

4.2.2. Eastlight will make sure that individuals are made aware of the identity of the data controller, the reasons why personal and sensitive personal data are required to be processed, how they will be processed, how they will be securely stored, disposed of and when we need their consent to share this information.

4.2.3. Individuals will be made aware that we may share data with third parties in line with our Tenancy Agreement, employment contract and/or privacy statements as well as the circumstances where this may happen and when any exceptions to this rule.

4.2.4. Individuals have rights under GDPR to request a copy of their personal data under Eastlight's Data Subject Access Procedure. Requests for information must be processed by Eastlight's Data Protection Officer.

4.2.5. In addition, Individuals have the following rights:

4.2.5.1. The right to request correction of their personal data if it is incorrect or out of date. We will aim to correct it as quickly as possible; unless there is a valid reason for not doing so, at which point they will be notified.

4.2.5.2. The right to withdraw consent for processing their data if the processing was

based on consent.

4.2.5.3. The right to request we delete their data, if they feel we should no longer be using their data. Upon receiving a request for erasure, we will confirm whether it has been deleted or the reason why it cannot be deleted (for example because we have a legal obligation to keep the information or we need it for a compelling legitimate business interest.

4.2.5.4. The right to object to processing of their data. They may request that we stop processing information about them. Upon receiving such request, we will contact them and let them know if we are able to comply or if we have legitimate grounds to continue to process your data. Please note, even after they exercise their right to object, we may continue to hold their data to comply with their other rights or to bring or to defend legal claims. We will allow individuals to opt out of direct marketing. This request will be acted upon as soon as we receive the request.

4.2.5.5. The right to request that we transfer their data to another data controller if the data is processed by automated means (This does not apply to paper files)

4.2.5.6. The right to request restriction of processing of their personal data. This enables the individual to ask us to suspend the processing of their personal data: (a) if they want us to establish the data's accuracy; (b) where our use of the data is unlawful but they do not want us to erase it; (c) where they need us to hold the data even if we no longer require it as they need it to establish, exercise or defend legal claims; or (d) they have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

4.2.5.7. Individuals may exercise their rights verbally, or by writing to us or by emailing us at DPA-FOI@eastlighthomes.co.uk

4.2.6. If Eastlight receives a request to exercise any of the above rights, we may ask the individuals to verify their identity before acting on the request; this is to ensure that their data is protected and kept secure.

4.2.7. Eastlight will review the data we process to ensure that all personal data held and processed by us is accounted for and recorded, alongside privacy impact assessments as to the scope and impact a data breach could have on data subject(s).

## 4.3. **DATA MINIMISATION**

4.3.1. Before collecting personal data, Eastlight will consider why it is needed, what information is being requested, how it will be used and how long we need to keep it for.

4.3.2. Eastlight will only collect personal information that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4.3.3. Eastlight's systems, processes and activities are designed to limit the collection of personal information to that which is relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

## 4.4. **DATA SECURITY**

4.4.1. Employees responsible for processing personal or special categories of personal data must make sure that it is used appropriately and kept both secure and confidential. They must always make sure that they only access and process data that they are authorised to manage on behalf of Eastlight.

4.4.2. If Eastlight works in partnership with other organisations or contracts out services/functions involving individuals' personal data, we will make sure data processors have relevant data processing contract obligations in place.

4.4.3. Deliberately obtaining or disclosing personal data unlawfully is an offence under the General Data Protection Regulations, which clearly states that any person must not knowingly or recklessly, without the consent of Eastlight as the data controller:

- obtain or disclose personal data or the information contained in personal data, or
- instruct another person to obtain or disclose the personal data or the information contained in personal data.

## 4.5. **DATA TRANSFER**

4.5.1. If records, manual or electronic, are taken from Eastlight's premises and/or published on any forms of public or internet sites this should be done in line with the security outlined in this policy, with the Data Protection Officer contacted if there are any queries regarding this.

4.5.2. Encrypted email or other secure data transfer system authorised by Eastlight's Data Protection Officer and ICT Services Manager must always be used when sending special categories of personal data electronically.

4.5.3. Users must take care when writing and addressing emails and uploading attachments to ensure the correct data is sent to the correct recipients.

4.5.4. If authorised to take company data off site to deliver a service, staff must ensure that only essential data is taken off site and appropriate measures are put in place to prevent unauthorised or unlawful processing and against accidental disclosure, loss, destruction or damage to data.

4.5.5. Employees should take a common-sense approach to keeping data as secure as possible when off site and lock hard copies of information away when it is not in use. Employees must never leave files in their car or vans overnight. Electronic personal data should only be stored on encrypted devices.

4.5.6. Eastlight will only transfer personal data to jurisdictions outside the European Economic Area (EEA) if it has a recognised and adequate level of protection for data protection purposes. Transferring data outside of the EEA requires relevant information governance and security compliance checks and the Data Protection Officer's approval.

## 4.6. **DATA RETENTION**

4.6.1. Eastlight will not maintain records longer than they need to, nor should we destroy records sooner than is required.

4.6.2. Eastlight has a Data Retention Schedule which captures retention periods as set out by the relevant laws, contracts and our business requirements. It will also be updated to adhere to the GDPR requirement to only hold and process personal information for as long as is necessary.

4.6.3. If data is required to be kept longer than the stated retention period, then a review will be carried out and reasons for extended retention will be documented.

4.7. **DATA DISPOSAL**

4.7.1. The method of disposal and destruction of information and records will be achieved via a range of processes, with the Data Protection Officer and ICT Manager contacted if there are any queries regarding this. The method of destruction must be appropriate for the type of data.

4.7.2. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

4.8. **DATA BREACHES**

4.8.1. Whilst every effort and measure are taken to reduce the risk of data breaches, Eastlight' has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

4.8.2. Eastlight may consider taking disciplinary and/or legal action where applicable if staff (service users), consultants, Board members, volunteers, representatives of Eastlight or contractors (third parties) engaged to carry out duties breach this policy.

## 5. STATUTORY AND REGULATORY REQUIREMENTS

5.1. To produce Privacy Impact Assessments – a risk assessment evaluating the use of data in projects.

5.2. To have the policy and procedures in place to define how staff and anyone who processes data on our behalf behave regarding data protection.

5.3. To be able to demonstrate that we are compliant with GDPR and carry out periodic compliance checks reporting back to Board.

5.4. To report data breaches to the ICO within 72 hours of their detection.

5.5. To ensure personal data is available, that systems are resilient, and that data can be restored in the event of an incident or loss.

5.6. For someone to fulfil the statutory role of Data Protection Officer, a senior person, with detailed knowledge of GDPR. They must be independent, with no conflict of interest between the requirements of GDPR and any other duties they may fulfil. They may not be subject to undue influence in the fulfilment of their duties and will report directly to the board on all matters related to GDPR.

## 6. REVIEW

6.1. Eastlight will review this policy annually, or as legislation changes.

## 7. DATE OF POLICY

7.1. May 2020

**Appendix A – Golden Rules**

# Keeping you, Eastlight and our customers safe.

- Keep a clear desk policy. Don't leave personal information on your desk. Keep it locked away when you are not working on it.
- Lock your computer screen when you are away from your desk.
- Dispose documents with Personal identifiable information using the Eastlight' approved disposal methods
- Confirm the identity of callers
- Do double check email addresses before emailing any personal information.
- Use encryption facility when transferring personal identifiable information to 3rd parties (Please ask IT how to do this)
- Don't collect more information than you need.
- Don't share more information than is needed; redact any irrelevant information as appropriate
- Don't hold onto information for longer than required; regularly audit and dispose of information as appropriate
- Don't leave personal information lying around for others to read
- Do record information factually; remember the notes you make could be released under a subject access request
- Don't discuss information where it can be overheard
- Don't discuss personal details with their family members or any third parties without the permission of the individual
- Don't save or email personal data to your personal email or to a personal device such as mobile phones, tablets or PCs
- Don't post personal data without ensuring it is addressed correctly
- Share personal information with other teams on "need to know basis" and securely
- Organisation shift by contributing to a data privacy friendly culture.

## Appendix B – Processing Special Category Data

### Special categories of Personal Data are defined in the data protection laws as:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where Eastlight processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations

### We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal data
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1)

Where Eastlight processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing.

## Appendix C – Data Protection Principles

The GDPR data protection principles state that personal data be: -

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- 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 regulation requires that Eastlight shall be responsible for, and be able to demonstrate, compliance with these principles.

## Appendix D – Legal Basis for data processing

At the core of all personal information processing activities undertaken by Eastlight, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

## Appendix E - Key Definitions

| | |
|---|---|
| Data | All personal and special categories of personal data which are:<br><br>• processed electronically, that is, on a computer, including word processing documents, emails, computer records, IT system, CCTV images, microfilmed documents, archived files or databases, faxes and information recorded on telephone logging systems<br>• processed and stored by computer bureau<br>• received by third parties or agents<br>• held in manual or 'hard copy' files that are structured (filed by subject, reference, dividers, content or in chronological order) and where individuals can be identified, and information easily accessed without the need for extensive searching<br>• information forming part of a manual medical, education, employment or housing and social services record recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. |
| Personal Data | Personal data is defined as any information relating to an identified of identifiable natural person.<br><br>An identifiable is one who can be identified, directly or indirectly, by reference to an identifier such as the following:<br><br>• a person's name<br>• address<br>• date of birth<br>• statement of fact<br>• any expression or opinion expressed about an individual<br>• minutes of meetings, reports, income recovery papers<br>• emails, files notes, handwritten notes, post-it-notes<br>• CCTV footage if the individual can be identified by the footage<br>• tenancy agreements<br>• employment references<br>• anti-social behaviour reports/statements<br>• Excel spreadsheets, databases and lists of people set up by code or tenancy reference number<br>• income<br>• employment history<br>• location data<br>• IP Address<br>• One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person |
| Special Categories of personal data | Any information relating to an individual's:<br><br>• racial or ethnic origin<br>• political opinions |

| | |
|---|---|
| | • religious or philosophical beliefs<br>• trade union membership<br>• genetic data<br>• biometric data<br>• health<br>• sex life or sexual orientation<br>• offences committed or alleged to have been committed by that individual<br>• any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. |
| Data Subject | A natural person (individual) who is the subject of data processing. |
| Data Controller | The person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data are, or are to be processed. |
| Data Processor | Any person (other than an employee of the data controller) who processes personal data on behalf of the data controller. For example:<br>• contractors<br>• printing and design companies<br>• agency staff<br>• cleaners<br>• confidential waste companies<br>• storage companies<br>• ICT and HR system providers<br>• payroll providers<br>• credit reference agencies. |