EAST MIDLANDS COMMUNITY LED HOUSING

EMCLH Data Protection Policy

Date policy approved:	**21 July 2020**
Policy reviewed by:	**EMCLH Board**
Policy last reviewed:	**n/a**
Date of next review:	**July 2021**
Delegated responsibilities:	**none**

Signed by:	

EMCLH
July 2020

EMCLH DATA PROTECTION POLICY

1. DATA PROTECTION

1.1 POLICY STATEMENT

As individuals, we want to know that personal information about ourselves is handled properly, and we and others have specific rights in this regard. In the course of its activities the Trust (East Midlands Community-Led Housing) will collect, store and process personal data about people and we recognise the need for correct and lawful treatment of this data

The types of personal data that the Trust may be required to handle include information about current, past and prospective employees, trustees, suppliers, customers and others with whom it communicates. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and other regulations (Data Protection legislation).

1.2 STATUS OF THE POLICY

This policy and any other documents referred to in it has been approved by the Directors of the Trust. It sets out the Trust's rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. All data users across the Trust must familiarise themselves with this policy and comply with it when processing personal data. Failure to follow this policy may result in disciplinary action being taken which could include dismissal.

1.3 DEFINITION OF DATA PROTECTION TERMS

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom the Trust holds personal data. **Personal data** means data relating to a living individual who can be identified from that data

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed.

Data users includes employees whose work involves using personal data.

Data processors include any person who processes or handles personal data.

Processing of information – how information is held and managed Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

2. DATA PROTECTION PRINCIPLES

Anyone responsible for collecting, processing and managing personal data must follow strict rules called data protection principles. This section provides an overview of each of the principles and how we will comply with them.

2.1 LAWFULNESS AND FAIRNESS

The Trust will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosure to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2.2 PURPOSE LIMITATION

The Trust will only process personal data for the specific purposes for which it was collected or for any other purposes specifically permitted by data protection legislation. The Trust will notify those purposes to the data subjects when it first collects the data or as soon as possible thereafter.

2.3 DATA MINIMISATION

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

2.4 ACCURACY

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy

of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

2.5 DATA RETENTION

Personal data should not be kept longer than is necessary for the purpose or purposes for which they were collected. The Trust will take all reasonable steps to destroy or erase from its systems, all data which is no longer required.

2.6 DATA SECURITY

The Trust will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. The Trust will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves. Contracts with data processors will comply with data protection legislation and contain explicit obligations on the data processor.

The Trust will have in place appropriate security measures:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

2.7 ACCOUNTABILITY

The GDPR includes provisions that promote accountability and governance. The accountability principle requires us to demonstrate that we comply with the principles and state explicitly that this is our responsibility.

3. RIGHTS OF DATA SUBJECTS

We will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct and implementing technical and organisational measures.

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-making processes that will significantly affect them.
- To not have significant decisions that will affect them taken solely by an automated process.
- To take action to rectify, block, erase, including right to be forgotten, or destroy inaccurate data.
- To have personal data provided to them in a structured, clear and understandable format.
- To object to any automated profiling that is occurring without consent.
- To request the supervisory authority to assess whether any provision of the GDPR has been breached.

4. TRANSFERRING PERSONAL DATA

The Trust will not transfer data to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. DISCLOSURE AND SHARING OF DATA

When receiving telephone enquiries, the Trust will only disclose personal data we hold on our systems if we are able to check the caller's identity to ensure that information is only given to a person who is entitled to it.

If a colleague is unsure about the caller's identity or where their identity can't be checked, they must ask the caller to put their request in writing. If colleagues feel that they are being bullied into disclosing personal information they can refer the caller to their line Manager.

6. SUBJECT ACCESS REQUESTS

Individuals have a right to access any personal data relating to them which are held by the Trust. A formal request from a data subject for information the Trust holds about them must be made in writing. Employees who receive a written request should forward it to their line manager immediately. Once a subject access request has been received the Trust must respond without delay and at the latest within one month of the request being received.

EMCLH
JULY 2020