

Data Protection - introduction

Trustees have a legal obligation to comply with the Data Protection Act 1998 and the new legislation, General Data Protection Regulations (GDPR), coming into effect on 25 May 2018. The new law updates data protection laws making them fit for the digital age and covering cyber security as well as giving more control over use of personal data.

It is the Almshouse Association's understanding that the GDPR will require all organisations that hold personal data about individuals must have written consent from the individual to store such data. There will also be a requirement for individuals to confirm they are willing to be contacted by the organisation electronically or by telephone or post.

The Data Protection Act 1998 requires every data controller (e.g. organisation) that is processing personal data, to consider whether they need to register with the ICO. Many Almshouse charities will be eligible for exemption from registration, Maldon Housing Association is registered.

If Maldon Housing Association uses CCTV, it must be registered with the ICO. On Maldon Housing Association's registration this is included, in preparation for any such time CCTV may be introduced.

The Data Protection Act 1998 requires that:

- information is collected only for one or more specified and lawful purposes and not processed for any other purpose
- it is kept secure
- it is adequate, relevant and up to date
- it is not excessive and kept only for as long as it is needed
- the person about which the information is held may have access to it on request.

Data should be collected and processed in accordance with a data protection policy which sets out the ways in which the charity will adhere to the requirements of the Data Protection Act 1998.

Trustees should ensure that their staff are adequately trained in data protection matters so that they are aware how to store and process personal information. Residents and any individuals about whom personal information is held, should know what the charity is doing with the information and with whom it will be shared.

- Personal data which includes sensitive information such as that listed below, would be regarded as a more serious breach if released:
- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade Union membership
- physical or mental health
- sexual life
- criminal proceedings or convictions.

It is an offence for a charity to fail to comply with its obligations under the Data Protection Act 1998. Data protection guidance for charities is available from the website of the Information Commissioner's Office: www.ico.gov.uk.

Data Protection Policy

Introduction:

The purpose of this policy is to enable the Maldon Housing Association to comply with the law (the DPA 1998) in respect of the data it holds about individuals.

The Charity Will:

- follow good practice
- protect residents, trustees, staff, volunteers and other individuals by respecting their rights
- demonstrate an open and honest approach to personal data and
- protect the Charity from the consequences of a breach of its responsibilities.

This policy applies to all the information that Maldon Housing Association controls and processes relating to identifiable, living individuals including contact details, test and exam results, bank details, photographs, audio and digital recording.

Data Storage and processing:

Maldon Housing Association recognises that data is held about:

- residents
- trustees
- staff
- volunteers
- and members.

This information is always stored securely and access is restricted to those who have a legitimate 'need to know'. Maldon Housing Association is committed to ensuring that those about whom we store data understand how and why we keep that data and who may have access to it. We do not transfer data to third parties without the express consent of the individual concerned.

Rights of individuals

All individuals who come into contact with Maldon Housing Association have the following rights under the DPA:

- a right of access to a copy of their personal data
- a right to object to processing that is likely to cause or is causing damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed and
- a right to claim compensation for damages caused by a breach of the DPA.

Archived records are stored securely and the charity has clear guidelines for the retention of information.

The Trustees recognise their overall responsibility for ensuring that the charity complies with its legal obligations. The Chief Executive and Supported Housing Manager are responsible as follows:

Roles and Responsibilities:

- briefing trustees on Data Protection responsibilities
- reviewing Data Protection and related policies
- advising other staff on Data Protection issues
- ensuring that Data Protection induction and training takes place
- notification
- handling subject access requests.

The Chief Executive will take responsibility for Employee data and the Supported Housing Manager will take responsibility for Resident data for the above. All trustees, staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their roles.

Significant breaches of these policies will be handled under disciplinary procedures.

Key risks to the safety of data control and process:

The trustees have identified the following potential key risks:

- breach of confidentiality (information being given out inappropriately)
- individuals being insufficiently informed about the use of their data
- misuse of personal information by staff or volunteers
- failure to up-date records promptly
- poor IT security and
- direct or indirect, inadvertent or deliberate unauthorised access.

The trustees will review the charity's procedures regularly, ensuring that the charity's records remain accurate and consistent and in particular:

- IT systems will be designed, where possible, to encourage and facilitate the entry of accurate data
- data on any individual will be held in as few places as necessary and trustees and staff will be discouraged from establishing unnecessary additional data sets
- effective procedures will be in place so that relevant systems are updated when information about an individual changes.

If a breach of data security is suspected or occurs the Data Protection Officer / Trustees should be notified immediately.

Subject Access Requests

Any individual who wants to exercise their right to receive a copy of their personal data can do so by making a Subject Access Request, ('SAR') to the Chief Executive, Supported Housing Manager or Trustees. The request must be made in writing and the individual must satisfy the above of their identity before receiving access to any information.

A SAR must be answered within 40 calendar days of receipt by the charity.

Collecting and using personal data

Maldon Housing Association typically collects and uses personal data in connection with the provision of the objects of the charity.

Maldon Housing Association will:

- not use any of the personal data it collects in ways that have unjustified adverse effects on the individuals concerned
- be transparent about how it intends to use the data and give individuals appropriate privacy notices when collecting their personal data
- handle people's personal data only in ways they would reasonably expect
- not do anything unlawful with the data.

Keeping Data Secure

The Charity will take all appropriate measures to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction. This means that:

- *personal files for residents, trustees, and employees and applications for accommodation will be kept in a locked filing cabinet at all times with access only by authorised staff*
- *trustees' details will be kept in a locked filing cabinet with access only by the Clerk*
- *electronic files containing personal data will be password protected and passwords will be changed on a regular basis*
- *backed up electronic data will be held securely on an alternative site or when off-site it will be encrypted, password protected and only accessed by named staff*
- *if any data is taken from the office (e.g. to work at home) the data must be held securely at all times whilst in transit and at the location the data is held.*

Retention of personal data

Personal Data will be retained as directed by the General Data Protection Regulations and Statute.

More information:

Full information about the Data Protection Act, its principles and definitions can be found at www.ico.gov.uk.