READING ALMSHOUSE CHARITY ('Charity')

DATA PROTECTION POLICY

Aim

The purpose of this policy is to enable the Charity to comply with the law (The GDPR and DPA 2018) 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 we control and process relating to identifiable, living individuals including contact details, bank details, photographs, audio and digital recording.

Data Storage and Processing

The Charity recognises that data is held about:

- residents and prospective residents
- trustees
- staff
- visitors to the Charity's premises (CCTV images)

This information is always stored securely and access is restricted to those who have a legitimate need to know. We are 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 the Charity 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
- 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.

Roles and Responsibilities

The trustees recognise their overall responsibility for ensuring that the Charity complies with its legal obligations. The Clerk (currently Kate Bessant) is responsible as follows:

- 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
- administering the registration with the Information Commissioner's Office
- handling subject access requests

All trustees and staff 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
- failure to up-date records promptly
- poor IT security
- 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 Clerk and 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 clerk. The request must be made in writing and the individual must satisfy the clerk 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

The Charity typically collects and uses personal data (eg contact details, medical information, employment history and financial information, although this list is not exhaustive) in connection with the provision of accommodation to people in need in the Reading area. The Charity collects personal data mainly in the following ways:

- by asking applicants for accommodation to complete paper forms
- by asking residents to give staff information verbally and by email
- by asking residents to complete paper forms
- by asking staff to complete paper forms and supply information by email
- by asking trustees to complete paper forms and supply information by email
- through use of CCTV at some entrances to the Charity's properties

The Charity 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 cabinet at all times with access only by authorised staff
- personal files for employees will be kept at the Clerk's home with access only by the Clerk
- trustees' details will be kept at the Clerk's home with access only by the Clerk
- access to the Manager's and Clerk's computers will be password protected
- electronic data will be backed up in the cloud and held securely and only accessed by the Manager, Clerk or the Charity's IT consultants
- if any data is taken from the office (e.g. the Manager taking residents' emergency contact details home over the Christmas period) the data must be held securely at all times whilst in transit and at the location the data is held
- CCTV live images will be viewable only by staff, trustees and system maintenance contractors (as far as possible with the live screen being situated in the office) and stored images will be accessible only to staff, trustees, systems maintenance contractors and to others for law enforcement purposes

Retention of personal data

The Charity will not keep personal data for longer than is necessary. This means that:

- a resident's file will be completely destroyed after one year of the resident leaving or passing away
- records of complaint/investigations concerning residents will be destroyed six years after the resident leaves or passes away
- application forms for unsuccessful applicants will be destroyed three years after the date of application
- trustees will destroy and delete all charity documents held within their own records five years after receipt, including all computer data and paper copies
- trustees' personal information (excluding contact details) will be destroyed one year after ceasing to be a trustee and contact details will be destroyed three years after ceasing to be a trustee
- staff personal files will be destroyed 6 years after employment ceases
- CCTV images will be stored for 25 to 30 days

This policy has been approved for issue by the Board of Trustees
15 MAY 2018