



Okehampton United Charities

Funding for the Community

Data Protection Policy

Introduction:

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

The Charity Will:

- follow good practice
- protect applicants, tenants, residents, trustees, staff, 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, test and exam results, bank details, photographs.

Data Storage and processing:

Okehampton United Charity recognises that data is held about:

- applicants
- tenants
- residents
- trustees
- staff
- and other individuals

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 Okehampton United 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 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. A data protection officer, currently the Clerk, is 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.

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 or trustees
- failure to up-date records promptly
- poor IT security and
- direct or indirect, inadvertent or deliberate unauthorised access.

The trustees will review the charities procedures regularly, ensuring that the charities 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 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

Okehampton United Charity typically collects and uses personal data in connection with the provision of providing housing, benefiting the inhabitants of the area of benefit and enabling Okehampton United Charity to meet its objects listed in its scheme. The charity collects personal data mainly in the following ways:

- by asking applicants for grants and accommodation to complete paper forms
- by asking applicants and residents to give staff information verbally.
- By asking applicants and residents to give staff information by email.

Okehampton United 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 applicants, residents, trustees, and employees and applications for grants and accommodation will be kept in a locked office at all times with access only by authorised staff and trustees
- trustees details will be kept in a locked office with access only by the Clerk
- electronic files containing personal data will be password protected and passwords will be changed on a regular basis

- biweekly backed up electronic data will be held securely on an alternative site. 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

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

- a residents file will be completely destroyed after seven years of the resident leaving or passing away.
- applicants files will be completely destroyed after seven years of the application being completed.
- records of complaint/investigations concerning applicants, residents, staff and trustees will be destroyed 10 years after the matter is resolved.
- 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 twelve months after receipt, including all computer data and paper copies
- trustees personal files will be destroyed seven years after ceasing to be a trustee
- staff personal files will be destroyed seven years after employment ceases.

More information:

Full information about the Data Protection Act, its principles and definitions can be found at the Information Commissioners Office.

Agreed Board of Trustees 27th January 2021 updated 12th June 2023.