

COMMUNITY FUTURES

# Data Protection Policy Statement

2024



COMMUNITYFUTURES.ORG.UK

# Data Protection Act 1998

Community Futures is fully committed to full compliance with the requirements of the Data Protection Act 1998 (as amended). The charity will therefore follow procedures which aim to ensure that all employees, trustees, service users, partners, stakeholders, tenants, contractors, consultants, funders or other servants of agents of the charity (collectively known as data users) who have access to any personal data held by or on behalf of the charity are fully aware of and abide by their duties under the Data Protection Act 1998.



## Statement of Policy

The charity needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include members of the public, current, past and prospective employees, clients and customers, funders, local authorities and suppliers. In addition the charity may be required by law to collect and use information in order to comply with the requirements of other legislation. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Community Futures regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the charity and those with whom it carries out business. The charity therefore fully endorses and adheres to the Principles of the Data Protection Act 1998.

## Handling personal/sensitive data

Community Futures will, through management and use of appropriate controls, monitoring and review:

- Use personal data in the most efficient and effective way to deliver better services
- Strive to collect and process only the data or information which is needed
- Use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted
- Strive to ensure information is accurate
- Not keep information for longer than is necessary or required as defined by law
- Securely destroy data which is no longer needed
- Take appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data)
- Ensure that information is not transferred abroad without suitable safeguards
- Ensure that there is general information to the public of their rights to access information
- Ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 1998

These rights include:

- The right to access their own personal information within 40 days of request
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information regarded as wrong information
- Ensure that the charity will have an officer specifically responsible for data protection in the council
- Provide guidance and training for all those requiring training at an appropriate level
- Ensure that any breaches of this policy are dealt with appropriately



## The Principles of Data Protection

The Data Protection Act stipulates that anyone processing personal data must comply with 8 principles of good practice. These principles are legally enforceable.

Summarised, the principles require that personal data:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
4. Shall be accurate and where necessary, kept up to date
5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Shall be processed in accordance with the rights of data subjects under the Act
7. Shall be kept secure, i.e. protected by an appropriate degree of security
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- That data
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions