Essential Needs

Data Protection Policy and Procedures

Introduction

During the course of our activities as a furniture re-use charity we will collect, store and process personal data about our staff, volunteers, members, donors and customers. The personal data, which may be held on paper or on a computer or other media, is subject to legal safeguards specified in the Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR) 2018.

About this policy

This policy and any other documents referred to in it sets out rules on data protection, the legal conditions that must be satisfied when we obtain, store and process personal data, and our procedures for protecting such data.
This policy does not form part of any employee's contract of employment and may be amended at any time.

Essential Needs is the data controller for the information held. Certain trustees, staff and volunteers will be personally responsible for processing and using personal information in accordance with the DPA 1998 and GDPR 2018. Staff, trustees and volunteers who have access to personal data, will be expected to read and comply with this policy.

Definition of data protection terms

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:
Data Controller – Essential Needs is the data controller and decides what personal information we will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Personal Data – Information relating to an individual person that identifies or could identify them

Sensitive Personal Data - includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express consent of the person concerned.

Data Subject/Service User – The individual whose personal information is being held or processed by Essential Needs.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998 and GDPR 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies.

The Data Protection Act 1998/GDPR 2018

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

Processed fairly and lawfully. - The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controller in the course of our business, we will ensure that those requirements are met.

Processed for limited purposes and in an appropriate way - In the course of our business, we collect and process the personal data set out in the data protection regulations. This includes data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, referral organisations).

We will only process personal data for the specific purposes set out in the data protection regulations or for any other purposes specifically permitted by the Act.

Adequate, relevant and not excessive for the purpose - Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

Accurate - Data, which is kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that is accurate. It is the responsibility of individuals to ensure that data held by us is accurate and up-to-date. Individuals should notify the charity of any changes in circumstance to enable personal records to be updated accordingly.

Not kept longer than necessary for the purpose - We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Processed in line with data subjects' rights - We will process all personal data in line with data subjects' rights, in particular their right to know:

Whether or not a data controller processes their data

The purposes of that processing

The recipient or category of recipient of that data

The period for which the data will be stored

The source of the data, if it is not collected from the subject

The existence of automated decision making

Essential Needs will provide this information by way of a privacy statement which will be displayed on our website.

Data subjects also have the right to:

Request rectification of incorrect data.
Be forgotten – the erasure of data where the original purpose no longer applies and where there are no additional public interest, public health or legitimate statistical, historical or archival reasons

Not to be subject to decision making based solely on automated processing of their data without safeguards.

Data portability – the right to a copy of the personal data held in a commonly used and machine-readable format.

Data Security
We take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We have procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be

transferred to another data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Laptops and Portable Devices
All laptops and portable devices that hold data containing personal data must be protected with a suitable encryption program.

Disclosure and sharing of personal information
We may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.
The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows us to disclose data (including sensitive data) without the data subject's consent.

We will ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, landlords, government bodies, and in certain circumstances, the Police. All staff, trustees and volunteers should exercise caution when asked to disclose personal data held on another individual to a third party.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (e.g. a member of staff or a service user has consented to us corresponding with a named third party);

2. where the disclosure is in our legitimate interests (e.g. disclosure to staff - personal information can be disclosed to other employees if it is clear that those members of staff require the information to enable them to perform their jobs);

3. where we are legally obliged to disclose the data.

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

• to safeguard national security*****;

• prevention or detection of crime including the apprehension or prosecution of offenders*****;

• assessment or collection of tax duty*****;

• discharge of regulatory functions (includes health, safety and welfare of persons at work)*****;

• to prevent serious harm to a third party;

• to protect the vital interests of the individual, this refers to life and death situations.

Those marked ***** indicate that requests must be supported by appropriate paperwork.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request.

Dealing with Subject Access Requests

Individuals have the right to access their personal data and supplementary information.

Under GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information

The right of access allows individuals to be aware of and verify the lawfulness of the processing we undertake.

GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Under GDPR individuals also have the following rights:

- the right to rectification
- the right to erasure
- the right to restrict processing

We will treat all access requests and requests to rectify, erase or restrict processing in the same way.

GDPR also gives individuals the right to data portability. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a data controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

On request we will provide the personal data in a structured, commonly used and machine-readable form. (Machine-readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.)

Data subjects must make a formal request for information we hold about them. Requests for access may be made verbally or in writing.

Employees who receive a verbal or written request should refer it to the Manager.

When receiving telephone enquiries requesting disclosure of personal data we will ask the caller to put their request in writing. Staff or volunteers should not be bullied into disclosing personal information.

Subject to satisfactory completion of a written request, we will respond within one month, ensuring that all data provided protects the interests of third parties by deleting any reference to them. A copy of the response should be retained for use in case of challenge.

We will provide a copy of the information held free of charge. However, we may make a reasonable charge when a request is manifestly unfounded or excessive. We may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.

We will provide the Information within one month of receipt. We may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If the request is made electronically, you should provide the information in a commonly used electronic format.

Period of storage
The period for which data will be stored depends upon the original reason for the data processing, our contract with the data subject and the legal rights and obligations that follow, and other legal requirements. The period will be calculated from the last date when we had a dealing with the data subject. In the first instance that period will be 6 years for all data subjects.

At the end of such period the data will be erased. Data in the computer system will be automatically erased and paper records will be shredded.

Data breaches

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that our reputation is not damaged through inappropriate or unauthorised access and sharing.

- We will report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will inform those individuals without undue delay.

We will keep a record of any personal data breaches, regardless of whether we are required to notify.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

What will we do if we have a data breach?

Containment and recovery

As soon as a data security breach has been detected or is suspected we will:

a) Inform the manager/board of trustees
b) keep a record using Appendix C
c) Identify and implement any steps required to contain the breach
d) Identify and implement any steps required to limit the damage of the breach
e) If appropriate inform the police/insurance office

Assessment of risk

All data security breaches will be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach will be assessed in order to identify an appropriate response. The checklist in Appendix A will be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

Notification of breach

We will consider whether any individuals, third parties or other stakeholders should be notified of the breach. This will depend on the nature of the breach. The checklist in Appendix B: Notification of breach checklist will be used to identify potential stakeholders who should be notified and to establish what information should be disclosed.

Evaluation and response

It is important to investigate the causes of the breach and evaluate our response. A brief report on the breach, how it was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written.

If a breach is likely to result in a risk to the rights and freedoms of individuals then the breach will be reported to the relevant supervisory authority within 72 hours.

If a breach is likely to result in a high risk (e.g. criminal activity such as fraud, or published in the public domain) to the rights and freedoms of individuals then we will also notify those concerned without undue delay.

We will also need to consider whether the data breach is a serious incident, and if so whether to report to the Charity Commission.

Policy Review

This policy is managed and reviewed as appropriate by the Manager and the Board of Trustees.

The policy will be reviewed if a weakness in the policy is highlighted, in the case of new risks, and/or changes in legislation.

APPENDIX A: SECURITY BREACH RISK ASSESSMENT CHECKLIST

a) What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)

b) How did the breach occur?

c) What type of data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)

d) How many individuals or records are involved?

e) If the breach involved personal data, who are the individuals?

f) What has happened to the data?

g) What is the timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)

h) Were there any protections in place? (e.g. encryption)

i) What are the potential adverse consequences for individuals? How serious or substantial are they and how likely are they to occur?

j) What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?

k) What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

APPENDIX B: NOTIFICATION OF BREACH CHECKLIST

WHO TO NOTIFY

The following (non-exhaustive) list identifies key external stakeholders who may require notification.

- Police – in the case of criminal activity
- Individuals whose data has been compromised
- Information Commissioner's Office (ICO) -
- Charity Commission
- Others – e.g. banks

WHAT TO SAY

Any notification message should not be sent too quickly, it is important that we understand the extent of the breach and are able to provide useful information, whilst at the same time if there are important steps that individuals need to take this should be communicated promptly.

We will consider including the following:

- Details of the what happened and when the breach occurred
- What data was involved
- What steps have been taken to contain the breach and prevent reoccurrence
- Advice on what steps they should take e.g. contact banks
- How will we help and keep them informed

APPENDIX C: DATA BREACH LOG

Date.Time	**ACTIVITY** Activity, Decision, Instruction or Briefing (A, D, I or B)	Action	Owner	Completed