TEMPLATE

MODEL DATA PROTECTION POLICY

This is a model policy and is intended for guidance only. Any group using this document should change it to meet their own specific circumstances.

The **Information Commissioner's Office** (**ICO**) **–** provides independent advice and guidance about data protection and freedom of information.

Regular updates can be found on their website www.ico.gov.uk

Last updated: 2013

TEMPLATE

MODEL DATA PROTECTION POLICY

1. Introduction

(insert name of org)needs to collect and use certain types of information about the Individuals or Service Users who come into contact with ***(insert name of org)***in order to carry on our work. This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998.

2. Data Controller

(insert name of org)is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

(insert name of org)may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows ***(insert name of org)***to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of a Individual/Service User or other person

c) The Individual/Service User has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

(insert name of org)regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

TEMPLATE

MODEL DATA PROTECTION POLICY

(insert name of org) intends to ensure that personal information is treated lawfully and correctly.

To this end, ***(insert name of org)***will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

c) Shall be adequate, relevant and not excessive in relation to those purpose(s)

d) Shall be accurate and, where necessary, kept up to date,

e) Shall not be kept for longer than is necessary

f) Shall be processed in accordance with the rights of data subjects under the Act,

g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

(insert name of org)will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements

- Ensure the quality of information used

- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data collection

Informed consent is when

- An Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

(insert name of org)will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, ***(insert name of org)*** will ensure that the Individual/Service User:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

5. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is ***(insert name of org)***responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

6. Data access and accuracy

All Individuals/Service Users have the right to access the information ***(insert name of org)***holds about them. ***(insert name of org)*** will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition**, *(insert name of org)***

will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice

- Everyone processing personal information is appropriately trained to do so

- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the ***(insert name of org)***Data Protection Officer:

Insert name and contact details of the Data Protection officer.

Signed: Position: Date: Review Date:

TEMPLATE

MODEL DATA PROTECTION POLICY

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information ***(insert name of org)*** 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.

Data Protection Officer – The person(s) responsible for ensuring that ***(insert name of org)*** follows its data protection policy and complies with the Data Protection Act 1998.

Individual/Service User – The person whose personal information is being held or processed by ***(insert name of org)***for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of ***(insert name of org)***, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self assessment guide will help you to decide if you are exempt from notification:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx

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

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

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

This pack has been adapted with permission from Voluntary Action Leicester Model Data Protection Policy.