**GDPR Policy**

| **Author: Magdalen Bartlett** |
| --- |
| **Revision description:** | **Version** | **Date issued:** | **Date reviewed:** |
| **n/a** | **1** |  |  |
|  |  |  |  |
|  |  |  |  |

**Purpose**

The General Data Protection Regulation 2018 (GDPR) strengthened and unified data protection for all individuals within the European Union from 25 May 2018. This policy reflects the provisions of the GDPR and the Data Protection Act 2018 (DPA).

**Related policy and procedures:**

**Introduction**

The policy explains United Response’s commitment to protecting personal data protecting information, information systems and processes handling information in such a way that the confidentiality, integrity and availability is maintained and enhanced as the organisation learns and matures.This will be achieved through a high-level approach to Information Governance, a systematic and consistent approach to risk management; and effective and efficient records management.

**Roles and responsibilities**

Afrocats is responsible for ensuring that Trustees, staff and volunteers are aware of this policy, the Information Governance framework, procedures and standards so that Information Governance becomes a part of business as usual for the organisation. Specific responsibilities can be found in the accompanying guidance notes.

All staff, whether permanent, temporary or contracted, consultants and volunteers are responsible for ensuring that they are aware of the requirements of them and that they comply with these on a day to day basis.

Additional responsibilities lie with the Chief Executive as Data Controller.

**Data protection**

Personal data may relate to:

* people we support and their families
* Staff
* those we do business with
* Our supporters and donors

Afrcoats need to collect and use certain types of information about people with whom it deals in order to operate. This information will be current, although it could be historical or information that might be used in the future to provide support.

Afrocats may occasionally be required to collect and use certain types of information of this kind to comply with the requirements of law. This personal information must be handled properly however it is collected, recorded and used –whether on paper, in a computer or recorded on other material –and that there are safeguards to ensure this is compliant with the GDPR.

Afrocats promote a culture of positive data protection, seeing it as a route to provide a quality service, rather than a blocker to effective service provision.

Afrocats is committed to the lawful processing of personal information, not only to satisfy the GDPR and DPA, but also to maintain confidence with those we have relationships with. To support this, we fully endorse and adhere to the principles of data protection, as enumerated in the GDPR and DPA and set out in Section 3 of the accompanying guidance notes.

In order to meet the requirements of the legislation we will:

* observe fully the conditions regarding the fair collection and use of personal data
* meet our obligations to specify the purposes for which personal data is used
* collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements
* ensure the quality of personal data used
* apply appropriate checks to determine the length of time personal data is held
* take the appropriate technical and organisational security measures to safeguard personal data
* ensure that personal data is not transferred outside the European Economic Area without appropriate safeguards

In addition, we will ensure that:all staff managing and handling personal information are:

* aware that they are contractually responsible to follow good data protection practice
* appropriately trained
* appropriately supervised
* aware of who to contact, should they have any queries or concerns.
* any questions from Data Subjects around how their data is being used will be answered promptly
* the methods for handling personal data are regularly evaluated and assessed data sharing is carried out under written agreement, clearly setting out the scope, limits and conditions for sharing
* any disclosure of personal data will be in line with agreed procedures
* the Data Protection Notification is regularly reviewed for accuracy

For additional requirements relating to third parties, transfer of personal information, subject access requests, data flow mapping, the information asset register and notification to the Information Commissioner.

**Our legal basis for using data**

We only collect and use personal data when the law allows us to. Most commonly, we process it where:

* have consent
* to process data in order to comply with applicable laws and regulations for processing

**How do we store data?**

Personal data will be stored on our secure cloud servers and CRM.

**How long do we keep data for?**

We will keep personal information only for as long as we need to and/or are required to. The criteria we use for determining these retention periods is based on various legal requirements; the purpose for which we hold data and whether there is a legitimate reason for continuing to store it (such as in order to deal with any future legal disputes).

Personal information that we no longer need is securely disposed of and/or anonymised so you can no longer be identified from it. We continually review what personal information and records that we hold, and delete what is no longer required

**Data sharing**

We do not share, sell or rent personal information to third parties for marketing purposes. However, we may disclose your personal information in the following circumstances:

* To other third parties who support our fundraising operations including payment and processing services
* Where we are under a duty to disclose your personal information in order to comply with any legal obligation, for example, where ordered by government bodies and law enforcement agencies.

**Transferring data internationally**

If we ever have to transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

**Rights**

Everyone has rights under GDPR in regards to how personal data is used and kept safe:

* Right to be informed about the collection and use of your personal data
* Right to withdraw your consent which allows us to collect, store and process your personal data
* Right to request a copy of the information that we hold about you.
* Right to ask us to erase your data.
* Right to know if your personal data is being shared with anyone other than the person to whom you have given your personal data
* Right to restrict us processing your personal data Right to object and complain
* Right to know if we are collecting personal data on you for the purposes of profiling you.

**Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you receive a complaint that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, this should be raised this with us in the first instance by contacting our CEO as the Data Controller

Alternatively, you can signpost complaints to the Information Commissioner’s Office:

* Report a concern online at<https://ico.org.uk/concerns>
* Call 0303 123 1113
* Or write to: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF