Privacy Standard
(Formerly Data Protection Policy)

Index

1. Introduction 3
2. Background 3
3. Compliance with the policy 4
4. Responsibilities 4
5. Fundamental rights 5
6. Lawful basis for processing 6
7. Data Security 7
8. Subject access requests 7
9. Special category data 7
10. Consent 8
11. Retention of data 8
12. Guidelines for staff 8
13. Details of the Information Commissioner 10
14. Review of this policy 10

Appendix 1 11

The Law 11

1. Introduction

1.1 This document sets out Age UK Sutton's (AUKS) policy on data protection and information governance. It provides an overview of AUKS's data protection requirements under the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

1.2 This policy applies to all individuals who have access to personal information that AUKS processes, including trustees, employees at all levels whether permanent or temporary, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners (collectively referred to as Age UK Sutton colleagues). This policy applies to Age UK Sutton and its Trading Company.

2. Background

2.1 At the heart of the GDPR are a set of rules known as the data protection principles. These principles require any organisation, corporation or governmental body that processes personal information to handle it safely. Any information collected from individuals must be:

2.1.1 processed lawfully, fairly and in a transparent manner

2.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes)

2.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

2.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

2.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

2.1.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.2 As well as these 6 principles, all organisations that process personal information are required to demonstrate how they comply with the GDPR – this is known as the accountability principle.

2.3 The GDPR provides stronger protections for more sensitive information - such as an individual's ethnic background, political opinions, religious beliefs, health, sexual life, criminal history or any kind of biometric information. It is enforced by an independent information commissioner (in the UK, this is the Information Commissioner's Office (ICO)), who can take action against any company or governmental body that fails to protect personal information, or that abuses its right to collect and hold that information.

2.4 Unauthorised disclosures of confidential information, or any data of a personal nature, can result in significant financial penalties under the GDPR; up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater.

3. Compliance with the policy

3.1 AUKS is the Data Controller for any personal data that is processed under the GDPR. Any deliberate breach of the Regulation may lead to disciplinary action being taken and, depending on the severity of the breach, may also lead to criminal prosecution being taken against AUKS or the individual responsible for the breach.

4. Responsibilities

4.1 All AUKS team members are responsible for the security of the data that they handle and are responsible for ensuring that the data is collected, stored and used (collectively referred to as "processed") in accordance with this policy, particularly the guidelines set out within this policy.

4.2 Individual people have some key areas of responsibility:

4.3 The **Board of Trustees** are ultimately responsible for ensuring that AUKS meets its legal obligations in regards to data protection

4.4 The **Systems and Insight Manager** is responsible for

4.4.1 Keeping the CEO and Senior Management Team updated about data protection responsibilities, risks and issues

4.4.2 Reviewing all data protection procedures and policies as required, in line with the Policy Scheme of Delegation and current and future data protection legislation

4.4.3 Handling requests from individuals to view the information that AUKS holds on them (referred to as a "Subject Access Request"), or to exercise any other rights afforded to them by the GDPR and DPA 2018

4.4.4 Handling data protection questions from staff and anyone else covered by this policy

4.4.5 Management and reporting of information incidents / breaches that occur

4.4.6 Ensuring all systems, services and equipment used in the processing of personal data have appropriate security procedures and protections in place

5. Fundamental rights

5.1 As well as the 6 principles that set out how personal information must be handled, under the GDPR individuals also have a series of fundamental rights in regards to how their information is processed. These rights are:

5.1.1 **The right to be informed** - individuals have the right to know what information we collect and store about them, why we collect the information and what we do with it

5.1.2 **The right to access** - individuals have the right to request a copy of any information that we store about them and we are required to respond to requests within 30 days (see **Subject Access Requests** below).

5.1.3 **The right to rectification** - If the information we store about an individual is incorrect, they have the right to have it corrected

5.1.4 **The right to erasure (aka "the right to be forgotten")** - Individuals have the right to request that we remove all personal information that we store about them. This can either result in information being anonymised, suppressed or erased, depending on the information that we hold

5.1.5 **The right to restrict processing** - Individuals have the right to restrict how we process their information if; (a) they are contesting the

accuracy of the information, (b) they believe the data has been processed unlawfully and they would prefer that we restrict the processing of the information instead of erasing it, (c) they believe we no longer need the information but want us to retain it in order for them to establish, exercise or defend a legal claim or (d) they have objected to our processing of the information and we are currently investigating the objection

5.1.6 **The right to data portability** - In some cases individuals have the right to request a portable copy of their information in a commonly used, machine readable format, such as a .CSV

5.1.7 **The right to object** - Individuals have the right to object to us processing their personal information

5.2 The rights available to individuals vary depending on the lawful basis used when processing their personal information. More information about this can be found on the ICO's website and the **Lawful Basis and Retention Schedule**.

6. Lawful basis for processing

6.1 Under the terms of the GDPR, organisations can only process personal information relating to individuals if they have a lawful basis to do so. The lawful bases available to organisations are:

6.1.1 **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose

6.1.2 **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

6.1.3 **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

6.1.4 **Vital interests**: the processing is necessary to protect someone's life.

6.1.5 **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6.1.6 **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6.2 AUKS relies on different lawful bases for different services and functions within the charity. Please see the **Lawful Basis and Retention Schedule**

for further information on the lawful bases and types of processing activity that AUKS works within.

7. Data Security

7.1 AUKS is responsible for ensuring the security of any personal information that we process. AUKS has the following security precautions in place:

7.1.1 On-site and cloud based backups of client records, including the overall Charitylog database

7.1.2 Multi-level user access restrictions on all databases

7.1.3 Virus protection and hardware firewalls

7.1.4 Lockable cabinets for paper records

8. Subject access requests

8.1 All individuals have the right to access any information that AUKS holds on them. When an individual makes a request to access the information we hold on them, this is called a Subject Access Request.

8.2 Subject access requests can be made to anyone within an organisation and can be made in any format, including in person, via social media or by email. Organisations have 30 calendar days to respond to valid Subject Access Requests and they must be provided free of charge, unless the request can be deemed as "excessive or manifestly unfounded". Before any information is provided, the Systems and Insight Manager will verify the identity of the person making the request. For further information, see the **Subject Access Request Procedure**.

9. Special category data

9.1 Special category data is information about an individual that may be considered more sensitive than other personal information. Under the GDPR, the following types of information are classed as special category data:

- Race
- Ethnic origin
- Political beliefs/opinions
- Religion
- Trade union membership
- Genetics

- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation

9.2 Organizations are required to have a lawful basis for processing personal information that is classed as special category; this is separate from the lawful basis that other personal information is processed under. For further information on the lawful bases that AUKS relies on, see the **Lawful Basis and Retention Schedule**

10. Consent

10.1 Consent should only be used as the basis for processing information in specific circumstances, such as to share information with an external organisation or to sign up for marketing communication.

10.2 Individuals have the right to withdraw any consents they have given for any processing they have given it for.

10.3 Further details relating to when consent is an appropriate lawful basis can be found in the **Lawful Basis and Retention Schedule**

11. Retention of data

11.1 AUKS is committed to storing and disposing of all personal information in a secure and responsible manner. Personal information will only be kept for as long as it is required to fulfil the purposes that the information was collected for. For further details of how long each type of information is retained for, please see the **Lawful Basis and Retention Schedule**

12. Guidelines for staff

12.1 All staff members and volunteers are responsible for compliance with the GDPR and must abide by these guidelines.

12.2 The following guidelines should be considered alongside the AUKS **Confidentiality Policy**.

12.3 These guidelines should be adhered to regardless of whether you are working inside or outside the AUKS office.

General:

12.3.1 Access to personal information must be restricted to only those who require it to carry out their roles within AUKS

12.3.2 In most situations, an individual's personal information must be treated as confidential and should not be shared with any other individuals or external organisation, including other Age UK's. Personal information can only be shared if the individual has given their explicit consent for their information to be shared, or if the act of not sharing the information puts the individual at significant risk of harm (for example, to protect against potential fraud or abuse). For details regarding breaching confidentiality in these cases, please refer to the **Confidentiality** and **Safeguarding** policies.

12.3.3 Passwords and user accounts must not be shared with anyone, including other staff members

12.3.4 Whenever asking for the clients consent for a specific type of processing (e.g. sharing relevant personal information with an external organisation) the date and type of consent (e.g. verbal or written) must be recorded on the client's electronic record, either on the GDPR tab or using the options on the Record a Contact screen. Any supporting documentation, such as "**Keep In Touch**" forms, should also be uploaded to the client's record, where appropriate. ***Details of consent given must not be solely recorded in the client's case notes.***

12.3.5 If you are unsure about any aspect of data protection, speak to your line manager or the Systems and Insight Manager

Data storage/security:

12.3.6 Paper documents should be securely locked away when not in use and should not be left where unauthorised people could potentially have sight of them

12.3.7 Unneeded paper documents should be disposed of securely using one of the shredders in the office or the confidential waste paper bags

12.3.8 Electronic documents pertaining to clients should only be stored on the client's Charitylog record and should not be stored permanently on laptops, PCs or mobile devices, or on Google Drive or any other cloud platform. Any scanned documents must be deleted from the computer they were scanned to as soon as they have been uploaded on to Charitylog.

12.3.9 If data is stored on removable media, such as USB sticks or CDs, these should be securely locked away when not in use. These should also not be left in places like car boots overnight.

12.3.10 Documents used to record incidental client information (for example, notes of names or phone numbers taken while taking a telephone message) should be treated as confidential and disposed of appropriately

12.3.11 Anti-virus software and firewalls are in place to help protect computers from unauthorised access – these protective measures must not be interfered with in any way. Any issues with them should be reported to the Systems and Insight Manager at the earliest possibility

Data accuracy:

12.3.12 Staff should check the accuracy of data with the individual it relates to whenever possible

12.3.13 Inaccurate data should be amended whenever the data is found to be inaccurate and incorrect data should be removed

12.4 All of the above guidelines apply to staff working in any capacity, regardless of whether or not they are working in or outside the AUKS offices.

13. Details of the Information Commissioner

You can contact the ICO through the following methods:

13.1 **Online:**
https://ico.org.uk

13.2 Telephone:
0303 123 1113

13.3 **Post:**
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

14. Review of this policy

This policy will be reviewed on a regular basis, or when new legislation requires. This policy was last reviewed in July 2018.

Appendix 1

The Law

- General Data Protection Regulation
- Data Protection Act 2018
- ICO Website