Age UK Kensington and Chelsea

Title	**Data Protection, Privacy, Subject Access and Confidentiality Policy**	
Policy author and owner	**CEO and Leadership**	
Date created	**26 November 2021**	
Date approved	**10 January 2022**	
Amended and updated	**Summary of change**	**Date**
Amended and updated on		
Amended and updated on		
Amended and updated on		
Amended and updated on		
Planned review date	January 2025	

Age UK Kensington and Chelsea

Policy - Data Protection, Privacy, Subject Access and Confidentiality

Overview

Age UK Kensington and Chelsea (AUKC) is committed to being transparent about how it collects and uses personal data of staff, clients, and volunteers and to meeting data protection obligations. This policy sets out the organisation's commitment to data protection and the individual rights for those whose data we hold.

To meet our obligations, we have robust and transparent procedures for gathering, processing and disposing of data, manage sensitive data carefully and respond to subject access requests in a timely fashion.

We restrict access to information to those that specifically require it and will only use information that is relevant in ensuring that we provide the most appropriate service to our clients.

Accordingly, we take the security of personal data seriously and have internal policies and controls in place to protect data against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed inappropriately other than in the context of the proper performance of duties.

The data we store will be securely archived and where necessary, anonymised to maintain confidentiality of the individual. In these circumstances, data will be retained for statistical purposes and not attributed to individuals.

We will provide our staff with information on how personal data is collected, used and disposed of. This begins with the recruitment stage and continues through the full employment life cycle.

For the purposes of this policy, the term confidentiality is the protection of information given by or about any individual seeking the assistance of or being employed by or volunteering with AUKC. We will deal with confidential information provided to us sensitively and in accordance with the principle of acting in the best interests of the client and the volunteer.

Principles

Our policy is based on the following principles:

1. We will process data lawfully, fairly and in a transparent manner; and

2. Personal data is only collected for specified, explicit and legitimate purposes. It will be processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing; and

3. We will keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay; and

4. That personal data is kept only for the period necessary for processing; and

5. We have appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage; and

6. Clients and their circumstances will only be discussed with family, friends, including those that may have Power of Attorney and organisations that may have health or safeguarding responsibilities.

Application

The policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees referred to as HR related personal data.

It also applies to the handling of sensitive information as it is relevant to the service of the client and only by those people involved in the care or management of them.

Standards

AUKC will:

1. Comply with both the law and good practice; and

2. Respect individual's rights; and

3. Be open and honest with individuals whose data is held; and

4. Provide training and support for staff and volunteers who handle personal data so they can act confidently and consistently; and

5. Notify the Information Commissioner in compliance with Data Protection register.

AUKC recognises that its main priority under the Data Protection Act is to avoid causing harm to individuals.

In the main this means:

1. Keeping information securely in the right hands; and

2. Holding good quality information that is accurate, relevant and up to date.

In addition to being open and transparent, we will seek to give individuals as much choice as is possible about the data held and how it is used.

Confidentiality is between the individual and the organisation. It is not between the client or volunteer and the individual worker. Information concerning a client or volunteer will solely be used to support the best interests of the client, for the protection of individuals or to ensure that an individual is fully supported in their volunteering.

The right to confidentiality may be overridden where there is evidence of:

1. The person or someone else being at risk; and

2. Danger to the community and/or of serious crime; and

3. A requirement by law.

All decisions to breach confidentiality must be dealt with on a case-by-case basis, agreed with a member of the Executive team and clearly recorded in the case file and on the Incidents Database.

Significant breaches of this policy will be managed within AUKC's disciplinary procedures.

Responsibilities

The Board of Trustees acknowledges its overall responsibility for ensuring that AUKC complies with its legal obligations. The Executive team has responsibility for ensuring that the Data Protection and Confidentiality policy is robust and for reviewing the policy periodically or where legislative changes are made.

The Data Protection Officer is the Chief Executive, with the following assigned responsibilities:

1. Briefing the board on data protection responsibilities; and

2. Reviewing Data Protection and related policies; and

3. Advising other staff on data protection issues; and

4. Ensuring that Data Protection induction and training takes place; and

5. Notification; and

6. Handling and, or appropriately delegating subject access requests; and

7. Approving unusual or controversial disclosures of personal data; and

8. Approving contracts with data processors.

All staff and volunteers are responsible for helping the organisation keep their personal data up to date and should let us know if data provided to the organisation changes. Individuals may have access to the personal data of other individuals and of our clients in the course of their employment. Where this is the case, we rely on individuals to help meet its data protection obligations to staff and clients.

Any employee who breaches this policy may face disciplinary action, which could result in dismissal for gross misconduct.

Legislation

This policy is based on UK legislation as follows:

1. Data Protection Act 2018; and

2. Health and Social Care Act 2001.

Procedure

AUKC has defined procedures in place for Subject Access requests as well as a procedure for sharing information with other agencies about individual clients.

Responsibility and Review of this Policy

Each policy will bear a front sheet summarising the date of approval, date(s) of any amendments and proposed date of review.

Responsibility for this policy rests with the Chief Executive (AUKC) and appointed Executive Lead. The policy was approved in January 2022. It is due for review in January 2025 or sooner if circumstances demand otherwise.