


AUKKC Data Protection Policy

Document Control Information

Version History			
Version	Date	Detail	Author
2.0	Oct 2015	Policy added to MDI. Full review of content scheduled	Richard Brine
2.1	Feb 2018	No update required	Sue Baker

Current Version	
Name of Group Approving the Document	N/A
Date of Group Approval	N/A
Date Added to Master Document Index	23/10/15
Review Date	01/02/2020
Version Number	2.0
Related Documents	
Author	Richard Brine
Service Unit	All
Consultation Tracking Sheet	No

Approval Signature			
Version	Date	Signatory (Print)	Signature
2.1	Feb 2018	Sue Baker	

AUKKC Data Protection Policy

CONSULTATION TRACKING SHEET

This document must be completed and accompany the document through the final ratification and authorisation process. A copy of this sheet should be included at the front of the final published policy.

Name of Document: AUKKC Data Protection Policy

Name of person / team / committee asked to provide feedback	Date feedback request sent	Feedback received (Y/N)	Feedback incorporated into Policy (Y/N)

Document History and Change Record

The following are registered holders of controlled copies of this document:

Position	Version
Business Manager (Management Representative)	2.0

Amendment History			
Version	Date	Amendment	Approved By
2.0	Oct 2015	Document control information added	Richard Brine
2.1	June 2019	1 st paragraph updated	

AUKKC Data Protection Policy**Data Protection Policy**

Age UK Kensington & Chelsea (AUKKC) acquires data about its staff, service users and volunteers in order to provide services. Such data is protected under the current Data Protection Act. Age UK Kensington & Chelsea has a principle by which it does not pass information on to other organisations unless it is required to under the law. AUKKC will always ask permission to share information where we consider this to be in the individual's best interest and will inform the individual when we have a statutory duty to share this information. Personal data will only be processed in accordance with the current Data Protection Act. You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the Privacy Notice.

Scope

This policy applies to all paid staff, volunteers and users of Age UK Kensington & Chelsea.

Purpose of policy

The purpose of this policy is to enable Age UK Kensington & Chelsea to:

- comply with the law in respect of the data it holds about individuals
- protect Age UK Kensington & Chelsea's users, volunteers, staff and other individuals

Policy statement

Age UK Kensington & Chelsea will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently
- Notify the Information Commissioner in compliance with the Data Protection register

Age UK Kensington & Chelsea recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals.

In the main this means:

- keeping information securely in the right hands
- holding good quality information (accurate, relevant and up-to-date)

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Age UK Kensington & Chelsea will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

AUKKC Data Protection Policy

Responsibility

Trustees:

The Board of Trustees recognises its overall responsibility for ensuring that Age UK Kensington & Chelsea complies with its legal obligations.

Data Protection Officer

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

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Team/Department managers

Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

Staff and volunteers

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. Significant breaches of this policy will be handled under Age UK Kensington & Chelsea's disciplinary procedures.

All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures. Data Protection will be included in foundation training for volunteers. AUKC will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

AUKC is moving towards a single database holding basic information about all users and volunteers. Departments will for the time being, however, continue to hold separate registers of their users, and volunteers may also keep separate information about those they are supporting.

AUKKC Data Protection Policy

AUKC's databases and server are accessible using a password only. It is the responsibility of each staff member to take all reasonable steps to ensure that personal data about users and volunteers stored on our computer systems remains confidential. The following safeguards should be made to prevent unauthorised access:

- Data about individuals that is recorded on the database should only be accessed by staff and volunteers in the course of their work.
- Computer screens should be angled so that they are not open to view by unauthorised people.
- The database and all documents containing personal data should not be left open when staff are away from their desks (e.g. for meetings or at lunchtime).
- Individual computers should be password protected.
- Staff should not share their password with other members of staff or volunteers.
- Mailing lists created for the purpose of mailshots should be password protected and deleted when the mailout is complete.
- Paper based files kept in secure lockable filing cabinets, keys to be kept in a safe location

Additional paper copies of personal data should be created only when absolutely necessary and shredded when no longer required.

These and any other manual records, including indexes and computer printouts, should be secured to avoid unauthorised access or amendment as well as against loss through accidental or deliberate damage and deletion by ensuring that they are locked away when not in use. Any paper or records showing personal data including phone numbers should not be left visible on desks when not in use.

Records should not be taken out of the building unless absolutely necessary. Where this is necessary, extreme care should be taken to ensure that no record is lost or damaged in the process. Archived paper records of users must be stored securely off site.

AUKC will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
- Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

AUKC will establish retention periods for at least the following categories of data:

- Users/Members
- Volunteers

AUKKC Data Protection Policy

- Staff

Subject access requests

Any subject access requests will be handled by the Data Protection Officer.

Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information. The required information will be provided as a copy of the records held unless the applicant makes a specific request to be given supervised access in person.

Data Collection

AUKC is committed to ensuring that, in principle, data subjects are aware that their data is being processed and:

- for what purpose it is being processed
- what types of disclosure are likely
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Staff: in the staff handbook
- Volunteers: in the volunteer handbook
- Users: when they sign up (on paper or by phone) for services.

Whenever data is collected, the amount of mandatory data collected will be kept to a minimum and Data Subjects will be informed what data are mandatory and why.

Consent will normally not be sought for most processing of information about staff if the data is being processed in the course of their work for AUKC. Staff details will only be disclosed for purposes unrelated to their work (e.g. financial references) with their consent. This consent may be given in writing or verbally.

Information about users and volunteers will only be made public with their consent (this includes photographs).

'Sensitive' data about members (including health information) will only be held with the knowledge and consent of the individual.

Direct Marketing

AUKC will treat the following unsolicited direct communication with individuals as marketing:

- seeking donations and other financial support
- promoting any AUKC services
- promoting events

AUKKC Data Protection Policy

- promoting sponsored events and other fundraising exercises
- sending out information about other local services that is felt to be of interest to the individual.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all AUKC marketing.

AUKC does not share lists with other organisations.

Policy review

This policy will be reviewed annually