Adopted: 25th April 2017
Amended: July 2018

DATA PROTECTION POLICY
Guidance and procedures

1 PURPOSE

1.1 This document is a short brief on the requirements of General Data Protection Regulations (GDPR). It also covers the procedures Age UK Cambridgeshire & Peterborough (AUKCAP) has adopted to comply with legal requirements, demonstrate that these procedures have been adopted, monitor our performance and encourage good practice.

AUKCAP aims to be open about the type and extent of the personal data it holds. This data will only be what is necessary to fulfil its objective of promoting the well-being of older people in the Cambridgeshire and Peterborough area. Our interpretation of the legislation will give priority to the interests of the data subject and addressing their needs.

1.2 GDPR applies to all our activities with or on behalf of older people and to the internal operation of the charity, including all data about our staff, volunteers and trustees.

1.3 We are all responsible to make sure we are aware of the requirements of the GDPR and AUKCAPs procedures. Other documents relevant to this subject are:

- Confidentiality policy and procedures
- Use of computers and social media networks
- Disclosure & Barring Checks Policy and Code Of Practice

2.0 SCOPE

The topics covered include:

- Information covered by GDPR
- AUKP as a data controller
- Holding and taking care of personal data
- Obtaining and using personal data fairly
- Recruitment & Personnel records
- Disclosure to a third party
- Requests for access to personal data
- Record keeping & disposal
- Monitoring our compliance with data protection.

3.0 WHAT IS COVERED BY GDPR

3.1 The GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). It applies to personal data. This is information from which a living individual can be identified, either directly or indirectly (from other information held).

3.2 Personal data does not have to be written and includes visual, photographic and other non-text data. This covers information held on computer, other electronic equipment, paper based records and other records (e.g. microfiche).

4.0 AUKCAP AS A DATA CONTROLLER

4.1 Organisations or individuals holding personal data are data controllers. Many data controllers including AUKCAP must notify the Information Commissioner that we are processing personal data. The Information Commissioner maintains a public register of data controllers.

4.2 The Data Protection Commission has a list of standard purposes. In addition, AUKCAP is registered for "any other purpose that is deemed necessary and appropriate to enable the charity to fulfil its objectives and be innovative and responsive.

4.3 The Chief Executive is responsible for ensuring there is a valid notification in the register of data controllers

5.0 HOLDING PERSONAL DATA

5.1 You are only allowed to use personal data for the purposes for which it was originally obtained. Personal information you hold must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- Must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a format which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processes. 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 organisations measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- 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 organisation measures.

5.2 *See Record Keeping Policy appendix 1, Retaining Records* for policy on time limit for retaining records.

5.2 Members of staff who, as part of their roles, are required to collect and maintain personal data must take good care of data which they hold. There are two types of security breach that AUKCAP must protect against: (1) unauthorised access (2) data getting damaged, lost or destroyed.

5.3 <u>Unauthorised access:</u>

- Personal information must be securely stored in a locked filing cabinet. Personal data must not be kept on the desk top unless it is being processed. Such data must be kept in a closed file folder when on the desk top. When receiving clients

or visitors no personal data must be visible on the desk top or computer screen. All work areas must be cleared of personal data before leaving the office.

- Staff, volunteers and trustees should only have access to personal information when this is reasonable, relevant and necessary to undertake their role within AUKCAP.

- Trustees do not have the right of access to client records, personnel files or other personal information unless this information is relevant to a complaint, grievance, disciplinary or other formal investigation.

- Very occasionally it will be necessary to remove personal information/case files or other documents from AUKCAP's premises. This may be to allow records to be referred to during a meeting or conversation or to make such records available for scrutiny by a service user. Great care must be taken to ensure the security of such papers. Files removed from the office will be placed in an envelope marked 'Private & Confidential' with AUKCAP's contact details on the outside and if it is necessary to leave files in a car they must be placed in the boot and not left on display. A note giving details of the file removed will be left at the office. Papers will be returned promptly.

- Password protection/ Restricted Access will be used to restrict inappropriate access to personal and sensitive information.

- When disposing of confidential manual files all information must be shredded.

5.4 Damage, loss or destruction: You must take reasonable steps to protect against the risks of damage, loss or destruction of personal information

- AUKCAP's IT Manager, in conjunction with our outsourced IT contractors will maintain backup procedures to protect against loss or damage as a result of computer failure.
- AUKCAP has software installed to protect against computer viruses. Our outsourced contractors operate 'real time' virus checks.
- Measures must be taken to ensure AUKCAP premises are protected from the risks of fire and theft as part of AUKCAPs risk assessment procedures.

6.0 OBTAINING AND USING PERSONAL DATA FAIRLY

6.1 As a data controller AUKCAP must ensure that the rights of the data subjects under the legislation are preserved. These rights are as follows:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decisions making and profiling.

This is done by:

- AUKCAPs notification to the Information Commissioner
- All service managers who obtain, store, use or destroy information must put in place measures to inform the data subject about personal information held by AUKCAP and obtain evidence of their consent (unless consent is obvious from

the context in which data is collected). For one-off telephone calls this can be done by recording a verbal notification. For more complex or on-going contact with AUKCAP, this should be confirmed in writing.

6.2 The following data protection notification must be included as a minimum requirement for service documents (note: separate arrangements apply to Trading Alliance activities).

"Age UK Cambridgeshire and Peterborough receive funds from various organisations, such as local authorities, district and parish councils, NHS and other charities, to deliver many of our services. In order to provide support to you as a service user and also demonstrate to those organisations who provide funds, we seek permission to store your personal details to ensure we comply with the General Data Protection Regulations. We may also need to forward your details, with your consent, to other organisations in order to seek further appropriate support for you. Any information stored will only be used for the purpose intended and will not be shared with any parties, other than those discussed and in exceptional circumstances; these will be destroyed when no longer required. Please tick the box below if you consent to us recording and sharing your details when require to do so.

I agree to the recording of my personal details □

I agree to my personal details being shared with other appropriate organisation, those organisations being …….. □

You can withdraw or change these consents at any time. Please contact adminservices@ageukcap.org.uk Telephone: 01354 691896
Write to: Administration Services, Age UK Cambridgeshire and Peterborough, County Office, 2 Victoria Street, Chatteris, Cambridgeshire, PE16 6AP"

6.3 There are additional requirements for **sensitive personal data.** This includes information about racial/ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, alleged or actual offences or proceedings relating to an alleged or actual offence.

All service managers who obtain use, store or destroy **sensitive personal data** must put in place measures to ensure that the data subject has given their explicit consent. This means that when verbal consent is given, this must be followed up by written confirmation.

7.0 RECRUITMENT AND PERSONNEL RECORDS

7.1 All applicants must be informed about how their personal data will be used. It is recommended that the following information is inserted:

"By signing and returning this application form you consent to AUKCAP using and keeping information about you or by third parties (such as referees) relating to your application or future employment. This information will be used solely in the recruitment process. For unsuccessful candidates the information will be destroyed within 6 months unless you have consented to extend this period".

7.2 All personnel records for staff and volunteers must be treated as sensitive personal information. Service managers holding personal data about staff or volunteers must

take particular care about the security of this information. Sickness and absence records must be held separately and securely.

8.0 DISCLOSURE TO A THIRD PARTY

Information can only legally be disclosed to a third party if it is fair under the terms of the General Data Protection Regulations.

8.1 All representatives of AUKCAP must obtain the consent of the data subject before disclosing personal information to a third party unless there are exceptional circumstances. You must carefully consider the risks and benefits of all disclosures, when these will be done without the consent of the data subject.

8.2 If the data subject has withheld consent to disclosure, personal information must not be disclosed to a third party unless there is an exemption that will legally permit disclosure (e.g. legal requirement, emergency). The Chief Executive must be notified of all cases where disclosure to a third party is planned to go ahead and the data subject has refused consent.

8.3 You must not access personal data without the authority to do so and you must not knowingly or recklessly disclose it to third parties without meeting the requirements below.

8.4 You cannot use data for direct marketing of any goods or services, if the data subject has told you not to.

9.0 REQUESTING ACCESS TO PERSONAL DATA

9.1 Data subjects can ask to see virtually all the personal data you hold on them, including manual files. AUKCAP has one month to comply with a request. AUKCAP will not normally charge a fee to comply with a subject access request. However, there may be circumstances, for instance if a request is manifestly unfounded or excessive, when the organisation feels it is necessary to charge a “reasonable fee” for the administrative costs of complying with a request. We may also charge a reasonable fee if an individual requests further copies of their data following a request. In this case the fee will be equivalent to the administrative costs of providing further copies.

9.2 When receiving a request it is important to assess whether it is fair to release the information when a third party is involved. Information can be edited or withheld to protect the identity of a third party. A third party can also be asked to consent to the disclosure.

10.0 RECORD KEEPING - STORAGE & DISPOSAL

10.1 Personal information can be held in a variety of documents and it is important to adhere to the recommendations for storage and disposal of each category of document. Guidelines for each category see Record Keeping Policy.

11.0 ENCOURAGING GOOD PRACTICE AND MONITORING COMPLIANCE

11.1 To ensure that AUKCAP develops good data protection practice, implementation of data protection procedures will be maintained and monitored by the Senior Management team.

11.2 All staff and volunteers who have contact with personal data will be briefed to understand their responsibilities for data protection.

11.3 AUKCAP will ensure staff and volunteers are aware that the charity monitors e-mail, social media and telephone use (see policy on use of computers and social media networks).

11.4 Breaches of data protection should be reported to your manager, recorded and investigated. Serious breaches of AUKCAPs guidance and procedures will be treated as a disciplinary offence.

12.0 MONITORING

This document will be reviewed within 36 months of adoption.

OTHER RELATED POLICIES

Confidentiality
Record Keeping Policy including Appendix 1 – Retaining Records
Financial Policy
Safeguarding Vulnerable Adults