Reviewed: October 2024

CONFIDENTIALITY POLICY AND PROCEDURES

PURPOSE

The confidentiality policy lays down the principles that should be observed by staff, Trustees and volunteers when conducting work on behalf of Age UK Cambridgeshire & Peterborough, to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

The dignity and choice of older people coming into contact with Age UK Cambridgeshire & Peterborough (AUKCAP) must be recognised and valued at all times. The right to privacy is essential to any service user so they have trust and confidence in the organisation and know they will be treated with respect and dignity.

Everything that is said to staff, Trustees and volunteers by older people should be regarded as confidential. Similarly, in Trustee, sub-committees and staff meetings, any discussion of older people and issues that have arisen should be regarded as confidential. Therefore, all matters should be treated as confidential.

SCOPE

This policy explains how confidentiality is maintained within the organisation and what to do when this poses difficulties and dilemmas.

POLICY

The principle of confidentiality covers any information concerning the internal affairs of AUKCAP and should be embraced equally by Trustees, staff and volunteers. There are several reasons for this policy:

- To protect people who contact us and those who use our services, who are employed by us or volunteer.
- To provide practical guidance to all AUKCAP representatives.
- To protect the charity and all AUKCAP representatives.

- To comply with the General Data Protection Regulations (GDPR; see separate Data Protection policy).

Board members, staff and volunteers will be informed of this policy when first joining the organisation and will be asked to sign that they have read and understood this and will abide by it. Each year they will be asked to sign a statement on their Annual Declaration to confirm they continue to understand the policy and will do so should they leave the organisation. Any contacts of the organisation must also adhere to this policy and will understand that a breach could result in further action.

USE OF INFORMATION

1 General enquiries

Enquirers can make a general approach to AUKCAP rather than an individual staff member or volunteer. As such, any information "belongs" to AUKCAP, not the individual staff member. Confidentiality does not prevent discussion between AUKCAP representatives in order to offer the fullest response to a request.

2 Marketing

Direct marketing including promotional activities are subject to the General Data Protection Regulations and The Privacy and Electronic Communications (EC Directive) regulations. No representative of AUKCAP can make unsolicited phone calls or send emails to someone who has told AUKCAP that they do not want correspondence from the charity. Permission must be sought and recorded for any marketing contact. All approved marketing by AUKCAP representatives must identify the sender and the name and address of the charity.

When individuals say they do not want to receive marketing materials this request must be dealt with promptly (see Privacy Policy for further details).

3 Trustees

Members of the Board of Trustees have a right to information held by AUKCAP and are responsible for the policies and procedures of the organisation. However, any such information will not be disclosed unnecessarily to Trustees unless such disclosure is

relevant and necessary. Individual Trustees will not elicit information of a personal nature except where it is relevant to resolving a defined task.

A record will be kept of all requests by Trustees to view a file containing details of a personal nature. The record will summarise the nature and scope of the information disclosed and the reason for the disclosure.

Given their rights of access it is vital that Trustees maintain strict confidentiality about the affairs of the organisation, its employees, users and anyone else involved with it.

Trustees are required to sign a copy of this policy agreeing to observe strict confidentiality about AUKCAP affairs, unless this is information that is (or can reasonably be expected to be) in the public domain. Breaches of this requirement may lead to a Trustee being required to resign from the Board.

4 Staff

Employees who hold a line management position may need to know confidential information about other staff members.

Access, storage and disposal of confidential information about employees is subject to the same principles as confidential information held by staff in respect of users.

Confidential information will therefore:-

- Be restricted to those who need to know.
- Access to electronic personnel files and records will be restricted to those who need to know.
- Paper records will be kept securely and disposed of appropriately.

5 Volunteers

A volunteers' pack is given to all new volunteers. This requires that they respect the privacy of users, maintain strict confidentiality about the affairs of the organisation and its employees and do not disclose to others information they have gained during their voluntary work. They are also required to sign to confirm they have read this policy which binds them to these conditions.

Information concerning volunteers is stored on Charity Log. Volunteers have a right to expect that information given to AUKCAP will be treated as confidential.

6 Additional requirements

In relation to some services (such as Information and Advice) there may be additional confidentiality requirements that apply to meet regulatory or good practice guidance.

LOCATION

Collecting personal information from service users should be carried out in privacy.

- Offices – Interview rooms should be used, wherever possible. Visitors should always be asked whether they wish to discuss their circumstances privately.
- Users Homes – Effort should be made to exclude people who have no legitimate interest in the information given. This includes anyone who the user does not want to be present, including spouses, children or their carers. If in doubt the interview should be postponed.
- Day Centres – Should take place away from main activities. Service users should always be asked whether they wish to discuss their circumstances privately and a separate room should be made available.
- Telephone – The conversation should take place with as much privacy as possible and where people who are not representatives of AUKCAP cannot overhear.

DISCLOSURE

Any information given by any service user must be used only for the purpose for which it is given and may not be released to another person without the permission of the user. However, a user may choose to waiver confidentiality if it is in their own interest to do so in which case information may be given to a third party. The user's consent can be provided in writing or verbally but must be recorded.

- Internally to another service
  When a service user is referred to another service within AUKCAP, they have a right to know and must give their permission, in writing or verbally, which will be recorded, for the referral.

- To another organisation or individual
  If it is necessary to disclose information to another organisation or individual, the person about whom the information is concerned, must give their permission before further action is taken. Consent will ideally be given in line with the organisations Consent Statement, however where not possible the statement will be shared verbally and verbal consent can be accepted and recorded, validating actions taken on an individual's behalf.

  Without this permission there is a breach of confidentiality because action would be taken without the knowledge or consent of the person and may not be in accordance with their wishes or in their best interests.

- Disclosure in exceptional circumstances
  Our commitment to respect individual choice, independence and privacy may pose difficulties and dilemmas for us. There may be situations where an AUKCAP representative has been unable to secure agreement of an individual to disclose information. The AUKCAP representative must always discuss proposals to involve a third party against the wishes of a user with their line manager or AUKCAP's Chief Executive.

  If after full discussion, it is decided that confidentiality should be broken the user must be informed immediately and reasons for our action should be explained.

- Renewing Disclosure
  In line with GDPR consent to store and share information must be sought on an annual basis and recorded electronically.

RECORDS

Background

AUKCAP is registered under the General Data Protection Regulations which forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). The Act gives protection against possible dangers arising from the use and storage of recorded personal information, both manual and computer held records.
(See Data Protection Policy for full details on holding and taking care of personal data).

Record keeping in practice

It is not always necessary to keep detailed records about enquiries, volunteers, staff or service users, but where there is a need to do so, the following procedures will apply:

- Records will be held securely
- Information on records should be as accurate as possible and the source of the information included.
- Only sufficient information relevant to the service or services being used should be kept, we should not record information surplus to those requirements.
- All records should be clear and factual. Personal observations about the character of the individual or their circumstances should not be recorded without supporting information.
- Unprofessional phrases, jargon, irrelevant speculation and offensive subjective statements will not be acceptable.
- Records should be reviewed at regular intervals and at least annually.
- Measures should be taken to ensure data is not altered, destroyed or disclosed.
- Service users, staff and volunteers have the right with reasonable notice, to view AUKCAP's records relating to them.

Handling of records outside of AUKCAP's premises

It will sometimes be necessary to take information away from the office e.g. contact details. Such notes should be destroyed after use. If paper files are removed from the office to take to meetings or to work on from home, great care will be taken to ensure the security of such papers.

Confidential papers should not be left unattended or on display. They should be returned to the office promptly.

CLEAR DESK

A clear desk reduces the risk of a security breach, fraud and information theft caused by documents or screens being left unattended in AUGECAP premises or home work stations.

At the end of a working day or when leaving their home/office work station, all employees are expected to tidy their desks of any paper files with personal information. Confidential documents should never be left unattended. All papers should be removed from printers/photocopiers for filing or disposal.

We should handle a piece of paper once – act on it, file it, or put it in the shredder.

Computer systems should be logged off, closed down and locked away with desks cleared at the end of each day.

Home work stations should be treated in the same way as a desk in AUKCAP premises.

RETENTION & DISPOSAL

Old records and files should be regularly monitored, and information destroyed when it is no longer appropriate to keep it. Any electronic files, papers, records containing names and addresses should, when no longer needed, be destroyed.
All paper personal information should be destroyed by shredding.

All records will ne held securely for the period of time as required by law. Please see Appendix 1 for Retaining Records

MAINTAINING CONFIDENTIALITY

- The Confidentiality Policy will form part of every staff member's statement of particulars of terms of employment. All staff will be required to confirm that they have read and understood the Confidentiality Policy and sign a declaration.

  Trustees and volunteers will be required to confirm that they have read and understood the Confidentiality Policy and sign a declaration.

- Breaches of confidentiality should be reported to the relevant line manager, recorded and investigated. Serious breaches will be reported to AUKCAP Senior Information Risk Owner and subsequently the Information Commissioner's Office if appropriate.

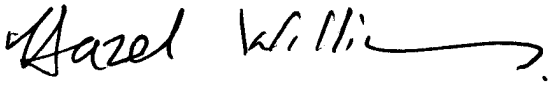
  Any member of staff, Trustee or volunteers found neglecting or misusing personal information will be subject to disciplinary procedures.

REVIEW

This policy will be reviewed every 24 months.

Confidentiality policy approved: October 2024

Signed by Chair of Trustees:



Appendix 1 Retaining Records

Type	How Long	Where	Responsible for Disposal (ie shredding)	Notes
DBS Disclosure	6 Months	Electronically stored on Sharepoint	Executive Assistant	See policy if need to keep individual record for more than 6 months
Client Files	7 years	Paper archives or Electronically stored on Sharepoint	Senior Leadership Team	Archived in clearly labeled archive boxes. Split into financial years
Financial Records	7 years	Archive	Senior Management Team	Must be clearly labeled Archive boxes. Split into financial years.
Volunteer Records	3 years	Charity Log	Organiser	
General Personnel Files	6 years	Paper archives or Electronically stored on Sharepoint	Senior Leadership Team (including Executive Assistant)	
Staff Diaries	7 years	Archived	Executive Assistant	Returned to Head Office annually with end of year financial paying in books – to be filed in archived year boxes
Payroll information	7 years	Archives & Sharepoint	Senior Leadership Team	
Unsuccessful Job Applicants	3 months	Sharepoint	Executive Assistant	