Confidentiality Policy

In the following, the word 'user' refers to anyone who uses the services of Age UK Surrey (AUKS) directly or indirectly, whether an individual or another organisation, including Age UK. 'Staff' refers to paid staff and volunteers. This policy should be read in conjunction with other relevant policies, in particular the Data Security Policy.

1. Introduction

AUKS recognises that the principle of confidentiality should apply to any information about its service users and the internal affairs of the organisation and its employees and should be adhered to by all Board members and employees.

AUKS service users have a right to privacy and confidentiality, and it is essential to ensure that users have trust and confidence in AUKS and are treated with respect and dignity.

Everyone will be made aware that their duty of confidentiality is a main term and condition of their Contract of Employment and will be asked to sign a statement of confidentiality indicating that they have read, understood, and will abide by this policy (Appendix 1). Board members and volunteers will also be asked to sign the statement of confidentiality. Confidentiality is not just a contractual requirement but a requirement under the Data Protection Act 2018.

2. Aim

The aim of this policy is to:

Ensure that users approach AUKS with trust and confidence.

Ensure that all Board members and employees of AUKS understand and carry out their duties to safeguard a user's rights to confidentiality by avoiding careless or wrongful disclosure of information entrusted to AUKS by the user.

Ensure that all Board members and employees of AUKS understand that their knowledge about internal affairs or the financial status of AUKS, its Board members and staff is confidential.

3. Practical Aspects

AUKS offers to its users a confidential advice service. It is implicit therefore that such confidentiality is respected.

An enquirer's approach is to the organisation rather than to individual employees or volunteers. Discussion of information with team members or volunteer of AUKS, who may be able to help with the query, does not breach confidentiality.

Under no circumstances should details of a client be discussed outside the organisation by anyone working on behalf of AUKS in such a manner that it is possible to identify the client. The exception to this is where written or verbal permission is obtained from the client first.

A caller may request that information should not be divulged to anyone else. This wish should be respected. The only exception would be where such information contravenes the law, endangers others, or in an emergency "life and limb" situation. **Confidentiality does not apply in possible cases of safeguarding**.

In safeguarding situations individuals should immediately consult their Line Manager, Safeguarding Lead or, in their absence, the Chief Executive, first advising the user that this action is necessary.

The user will have the right to complain if information is divulged without their permission. The complaint will follow the procedure set out in the Complaints Policy of AUKS.

The Chief Executive of AUKS will monitor the effectiveness of this policy and bring it forward for review at least every three years.

4. Procedures to be followed

Under no circumstances should details which enable an individual to be identified be made public or passed to a third party without the user's informed consent - verbally, or in writing if the situation is felt to warrant it.

Wherever possible, a signed consent form will be completed by the client to ensure that they have given informed consent on how their data will be used. In many cases, such as telephone advice or one-off enquiries, where this is not possible and is not needed in order to progress the case (e.g. for liaison with third parties), verbal consent will be recorded on the client record.

Such consent is valid only for the purpose for which it was given. If information is to be re-used in a different context, permission should be sought again.

If an individual does not have mental capacity to give permission, it should be sought from their carer, relative or advocate and only with the consent of the Chief Executive or member of staff with authority to deputise.

5. Enquiries Involving Third Parties

Correspondence from AUKS on behalf of a service user should make it clear that the reply will be shown to the user. In the event of a response being received from a third party that would, in the opinion of AUKS, damage relations or negotiations with the user, AUKS should check with the other agency that the answer could be shown to the user.

The situation often arises where an enquiry is made on behalf of someone by a third party, e.g. by a relative, friend, neighbour for an elderly person. Confidentiality is not broken if information is given to be passed on but, whenever possible, this should be backed up with a relevant leaflet, factsheet or handout, to ensure that the information ultimately received by the third party is accurate.

Where it is agreed that AUKS will contact a third party on behalf of a client, the client must give consent. This should be recorded on the client's record.

A new consent form must be signed each time a new issue/case is opened, e.g. where a client returns for further advice or advice on a different matter after a previous case has been closed.

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

In cases where an enquirer acting on behalf of someone else is in possession of documents suggesting that they are acting with full knowledge and consent of the third party, great care

should be taken and the employee/volunteer should consult the Chief Executive if there is any doubt that the confidentiality rule could be breached.

6. Keeping and Safeguarding Records

Records relating to service users are available to relevant employees and volunteers who have undergone specific training and who have signed the statement on confidentiality.

Care must always be taken to ensure that all records are handled with discretion and are secured when the premises are not staffed. Correspondence and other records, minutes, files, card index systems pertaining to an individual or organisation should not be left on desks or in places where access to the information cannot be controlled. Notes should be destroyed once case files/data base records have been compiled.

All employee, volunteer and client paper records should be stored in locked cabinets and under GDPR everyone has the right to see their own files on request.

Old records and files should be regularly monitored and information destroyed when it is no longer necessary to keep it. Information on time limits for file retention is set out in the Control of Records Procedure (Staff Handbook/Procedures).

The same principles should be applied to confidential information in memos, briefing papers and minutes of meetings.

7. Use of Telephone

It is important that care is taken over the use of the telephone. Care must also be taken to prevent a personal caller from hearing or witnessing a conversation with another service user. Where two or more conversations are simultaneously taking place on telephones, staff must ensure that confidentiality is not breached.

When calling a person back, staff must check that the person they want is the person they are speaking to **before** divulging information about the person or stating they are from AUKS.

8. Removal of Information from the Premises

It is sometimes necessary for employees or volunteers to carry confidential information with them on home visits, or when attending meetings or case conferences. In these situations every effort must be made to ensure such material is kept to a minimum, is safe and in their possession at all times. Particular care should be taken with diaries where appointments indicate the name and address of a service user. Such material/information must not be left unattended in a vehicle during visits etc.

Papers relating to individuals must, when no longer needed, be returned to the office and destroyed securely when appropriate.

9. Information from Other Organisations

When receiving confidential or sensitive information relating to other Age UK/Age Concern groups or other organisations the same standards of confidentiality should be adhered to, as is the case with individuals approaching AUKS. Such information should only be divulged, if appropriate and properly consented, to a colleague or third party within the organisation, and never to anyone outside without consultation with the Chief Executive.

When in doubt about how to handle any information received, staff should contact a senior colleague or manager and inform them of the position.

10. Board Members

Board members will be expected to make themselves aware of this policy.

In respect of confidential agenda items at meetings and confidential minutes, Board members will be expected to adhere to the policy and guard against any breaches intentional or unintentional.

Where there may be a conflict of interest between providers who are Board members, some matters will remain confidential and the procedure at meetings may therefore exclude individuals who seem to have an 'interest'.

11. Breach of Policy

Any breach of this Policy may result in disciplinary action and could lead to dismissal.

12. Review - This policy will be reviewed every three years.

Issue	**Date agreed by Board of Age UK Surrey**	**Reviewed**
2	5th April 2011	April 2014
3	17th July 2014	July 2017/July 2019
4	24 September 2019	Aug 2023
	Date agreed by the Governance Committee of Age UK Surrey	
5	31st October 2023	

Appendix 1

STATEMENT OF CONFIDENTIALITY

I confirm that I have received a copy of Age UK Surrey's Confidentiality Policy and that I have read and understood it and will abide by this policy now and when I have left this organisation.

I declare that, at all times:

a. I will keep confidential any personal employee/client/user/volunteer information I receive, or to which I have access, and will not disclose it without permission and that

b. I will keep confidential any information about conduct, proceedings or the financial status of Age UK Surrey and its staff, paid and unpaid.

Signature: ……. Date: ……