Confidentiality Policy

Index

Version 1: Dec 2010; V2: January 2012
V3: May 2014; V4: February 2015;
V5: May 2016; V6: July 2018

1. Introduction

1.1 Confidential information is any information that could be regarded as 'personal'. It is information that is told to an individual or a group of people and is not meant for public or general knowledge. It is the duty of colleagues not to reveal to any other person outside the person(s) dealing with the case within the organisation any matter which becomes known to the individual through their involvement with the organisation.

1.2 This **Confidentiality Policy** has been drawn up to meet the needs of the organisation, its Board of Trustees, members, staff, volunteers and service users. Confidentiality should be maintained to protect all parties.

1.3 The object of the policy is to detail standards that all persons working for us or on our behalf, including trustees, employees at all levels whether permanent or temporary, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners (collectively referred to as Age UK Sutton colleagues) must adhere to and which are incorporated as part of normal working practice.

1.4 The most common situation where issues of confidentiality may arise will be matters relating to an individual's personal problems or circumstances. However, principles of confidentiality also relate to information concerning organisations outside Age UK Sutton itself, such as Age UK. The policy is designed to cover all aspects.

1.5 Board of Trustee members, staff and volunteers will be made aware of this policy when first joining the organisation and will be expected to understand and abide by it.

1.6 In the case of employees, their contracts will state the necessity of adhering to this policy and will make it clear that a breach could be a serious disciplinary matter.

2. General principles

2.1 Age UK Sutton recognises that colleagues gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from your line manager.

2.2 Colleagues are able to share information, such as details of any case work, with their line manager in order to discuss issues and seek advice.

2.3 Colleagues will avoid exchanging personal information or comments about individuals with whom they have a professional relationship.

2.4 Talking about the private life of an individual is to be avoided at all times, unless the individual in question has instigated the conversation.

2.5 Colleagues will avoid talking about organisations or individuals in social settings.

2.6 Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an appropriate member of staff, in the case of an organisation.

2.7 There may be circumstances where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. The CEO's consent must be sought before discussing the situation, unless the colleague is convinced beyond doubt that the organisation would not object to this. Alternatively, a discussion may take place with names or identifying information remaining confidential.

2.8 Where there is a legal duty on Age UK Sutton (AUKS) to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made (please see section 6: Breaching Confidentiality for further details).

2.9 Information about ethnicity, disability or any other sensitive information of citizens is collected in accordance with the Age UK Sutton **Privacy Standard** and the accompanying **Lawful Basis and Retention Schedule**.

2.10 AUKS handling of confidential personal information, as well as other aspects relating to confidentiality, will:

2.10.1 Promote, support and protect the privacy, dignity and rights of AUKS clients

2.10.2 Be understood by clients who have capacity, trustees, staff, volunteers and partner services

2.10.3 Comply with best practice

2.10.4 Conform with the law

2.10.5 Promote the care and welfare of clients and the effective operation of AUKS services.

3. Access to information

3.1 Information is confidential to Age UK Sutton as an organisation and may be passed to colleagues, line managers or trustees to ensure the best quality service for users.

3.2 Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.

3.3 Colleagues will not withhold information from their line manager unless it is purely personal.

3.4 Service users may have access to a paper or electronic copy of the information Age UK Sutton holds on them. Requests can be made to any member of the organisation and must be brought to the attention of the Systems & Insight Manager at the earliest possibility. For more information, see the **Subject Access Request Procedure**.

4. Maintaining security of information

4.1 When photocopying or working on confidential documents, colleagues must ensure people passing do not see them. This also applies to information on computer screens and other electronic devices.

4.2 When carrying paperwork outside of the office, best measures should be taken to ensure the security of the information and it should be returned to secure storage as soon as possible.

4.3 When accessing information outside of the office, such as when using a laptop or mobile phone, it is important to make sure the device is password protected and locked away when not in use.

5. Storing information

5.1 General non-confidential information about organisations is kept in locked filing cabinets and in computer files with open access to all Age UK Sutton colleagues.

5.2 Personnel information on employees, volunteers, and other individuals working within Age UK Sutton will be kept in lockable filing cabinets and will be accessible to the CEO and appropriate staff members as set out in the Scheme of Delegation.

5.3 In an emergency situation, the CEO may authorise access to files by other people.

6. Breaching Confidentiality

6.1 The limits to confidentiality must be explained to the client before gathering information from them.

6.2 Confidentiality can only be breached:

6.2.1 In exceptional circumstances, if the service believes that it is necessary to breach confidentiality in order to protect a person in an extremely dangerous/life threatening situation.

6.2.2 In order to safeguard the individual, such as in situations where the individual may be the subject of abuse or self-neglect (see the **Safeguarding Policy** for further details)

6.2.3 In exceptional circumstances, if the service, having made every effort to do so, still lacks the ability to interpret the person's method of communication, and is therefore unable to consult them in such a way as to elicit their views or involve them in a potential breach.

6.2.4 If people working within the service would otherwise be assisting a criminal offence.

6.2.5 If there is a court order for disclosure

6.3 When confidentiality has to be breached without permission, wherever possible and appropriate the member of staff shall inform the person at the earliest opportunity of the reasons for doing so, giving them opportunities to discuss other alternatives and to plan for likely outcomes. Every effort should be made to ensure the person is given the maximum control possible over the process of breaching confidentiality, and to keep them informed at every stage of any action that AUKS intends to take.

6.4 Service staff are not authorised to make the final decision about whether confidentiality is to be breached, unless in an emergency or in exceptional circumstances if they are unable to contact any senior manager within the service or within the wider organisation.

7. Procedure for breaching confidentiality within office hours

7.1 Any information from any source which gives rise to concern for the safety or wellbeing of a person or people, directly or indirectly, should be made known to the worker's Line Manager immediately.

7.2 Managers should ensure that their staff are aware of how to contact them, or a colleague at a management level, in an emergency during the working day and out of hours, including ways of interrupting meetings.

7.3 If an immediate Line Manager is unavailable, the concern should be escalated by the member of staff in possession of the information up through the infrastructure of the organisation, or to the Systems and Insight Manager.

7.4 Any decision to take further action will be made by the relevant Manager. This may be following discussion with the Chief Executive Officer (CEO) or other Senior Management Team members.

7.5 In circumstances where information has been received/actions observed indicating people other than clients of the organisation are at risk of harm, this information may be passed by a senior manager to relevant agencies, without identifying the source of information.

8. Procedure for breaching confidentiality outside of normal office hours

8.1 Emergency contact numbers for managers can be found in the staff directory.

8.2 These numbers are only to be used in circumstances where information has been received/observed which may require disclosure of information to relevant authorities or in other emergencies as set out in the **Business Continuity Plan**.

9. Disclosure and Barring Checks

9.1 Age UK Sutton complies fully with the Disclosure and Barring Service Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

9.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

9.3 Documents will be kept for 6 months and then destroyed by secure means. Photocopies will not be kept. However, Age UK Sutton may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

10. General Data Protection Regulation & Data Protection Act 2018

10.1 Information about identifiable individuals, whether on computer or on paper falls within the scope of the General Data Protection Regulation and must comply with the data protection principles. These are that personal data must be:

10.1.1 processed fairly, lawfully and transparently in relation to individuals;

10.1.2 collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with the exception of processing for the purposes of archiving in the public interest, scientific or historical interest);

10.1.3 adequate, relevant and not excessive;

10.1.4 accurate and, where necessary, up to date;

10.1.5 kept in a form which permits identification of data subjects for no longer than is necessary for the original purposes of the processing;

10.1.6 processed in accordance with the GDPR and in a manner that ensures appropriate security of the personal information

10.2 Colleagues accessing unauthorised files or breaching confidentiality may face disciplinary action.

10.3 For more information regarding Data Protection, refer to the **Privacy Standard**.

11. Whistle blowing

11.1 All colleagues hold the right to inform either his / her manager or one of the trustees if they believe that Age UK Sutton is being brought into disrepute by the actions of another colleague or Trustee, even if doing so could breach confidentiality. Further details can be found in the Age UK Sutton **Whistleblowing Policy**.

12. Advice/Information Enquirers

12.1 Age UK Sutton offers its customers a confidential advice service. It is implicit therefore that such confidentiality is respected.

12.1.1 An enquirer's approach is to the organisation rather than to an individual employee or volunteer; discussion in order to best serve the needs of the user does not breach the policy if such discussion is with another member of staff/volunteer.

12.2 In no circumstances should details of a service user be discussed with anyone outside the organisation, unless the act of not sharing details/information would put the individual at risk of harm.

12.3 Age UK Sutton aims to provide direct services to its customers. However, the user may choose to waive confidentiality if it is in his/her interest to do so, in which case information may be passed to an agreed third party with the individual's permission.

12.4 Age UK Sutton works closely with Adult Social Services & Housing (ASSH) and other agencies. Health & social care agencies provide funding for some of our services and with the consent of clients we may pass information between these organisations. This cuts down duplication of information and questions that service users are asked at assessment when they approach us to use our services for support. Where a user requests that information is not divulged to a third party this wish should normally be respected except in the situation where the individual or someone else may be at risk. In all such cases this should be discussed with the line manager.

13. Procedures to be followed

13.1 Colleagues faced with a decision relating to confidentiality must consult their line manager or a senior manager informing them of the situation. They must first advise the user that this action is necessary.

13.2 In most circumstances details which enable an individual to be identified should not 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

13.3 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.

13.4 If a person lacks mental capacity under the Mental Capacity Act 2005 and is unable to give permission then anything done for or on behalf of a person who lacks mental capacity must be done in their best interests.

13.5 If making a decision or acting on behalf of a person who lacks capacity you must consider whether it is possible to decide or act in a way that would interfere less with the person's rights and freedoms of action, or whether there is a need to decide or act at all. Any intervention should be weighed up in the particular circumstances of the case.

13.6 Employees who are dissatisfied with the conduct or actions of other colleagues of Age UK Sutton should raise this with their line manager. They should use the informal complaints process and not discuss their dissatisfaction outside of the organisation.

13.7 Information sharing and respecting confidentiality falls within the guidance set out in the Mental Capacity Act Code of Practice 5.56 -5.57 for people assessed as lacking capacity to give consent and provides a clear framework for AUKS staff to work to.

13.7.1 All decisions should be recorded whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures.

13.7.2 If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with AUKS's own retention policy, the information should not be kept any longer than is necessary. In some circumstances this may be indefinitely; in these cases, retention should be periodically reviewed, in line with the **Lawful Basis and Retention Schedule**.

14. Enquiries involving Third Parties

14.1 Correspondence from Age UK Sutton 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 which would in the opinion of Age UK Sutton damage relations or negotiations with the user, Age UK Sutton should check with the agency that the reply can be shown to the user

14.2 A situation can often arise where an enquiry is made on behalf of someone else (third party), e.g. by a relative, friend or neighbour. Wherever possible any response provided to the third party should be backed up with a relevant leaflet, factsheet or hand-out, to ensure that the information ultimately

received by the third party is accurate. Care should be taken not to disclose confidential information in these circumstances.

14.3 When supporting someone who claims to bea n appointee or to have power of attorney over an individual, documentary evidence of the specific powers granted to the attorney should be sought before sharing any information regarding the donor.

14.4 In cases where it would be helpful for Age UK Sutton to contact an outside agency, the client / third party should be asked for written consent. If this is not possible, telephone consent is acceptable but it must be logged and dated on Charitylog. Without this consent there is a breach of confidentiality, as action would have been taken without the knowledge or consent of the client / third party and may not be in accordance with their wishes or in their best interests.

14.5 In cases where an enquirer acting on behalf of someone else is in possession of documents suggesting that he/she is acting with full knowledge and consent of the third party, great care should be taken and the employee/volunteer should consult the CEO if in any doubt that the confidentiality rule could be breached.

15. Keeping and Safeguarding Records

15.1 Records relating to service users are available to staff/volunteers who have undergone selection and training.

15.2 Care must be taken at all times by Trustees, staff and volunteers to ensure that all records are handled with discretion and are secured when the premises are not staffed. Correspondence and other records, minutes, files, database appertaining to an individual or organisation should not be left on desks and notes should be destroyed once case files/database records have been compiled. Appointment diaries and any other documentation which contains personal information should be left in the office at weekends and holiday periods and stored securely when taken out of the office.

15.3 All paper enquiry records should be kept in lockable cabinets if they cannot be transferred on to Charitylog, with access limited to relevant staff.

15.4 Old records and files should be regularly monitored and information destroyed when it is no longer necessary to keep it. Files, papers, records containing names and addresses should, when no longer needed, be

shredded/anonymised. Please refer to **the Lawful Basis and Retention Schedule** for further information.

16. Removal of Information from the Premises

16.1 It is sometimes necessary for staff to carry information relating to clients with them on home visits or when attending meetings or case conferences. Staff are expected to exercise due care and attention to ensure that such material is kept to a minimum, is safe and in their possession at all times. Particular care should be taken with diaries and other documentation where appointments indicate the name and address of a service user. No such material/information should be left unattended in a vehicle. Papers should be returned to the office as soon as possible and always before the end of the working day.

16.2 Electronic devices used in community work should be password protected and stored securely. The includes smartphones, tablets, laptops and USB or other external storage devices

17. Organisational Information

17.1 Staff, volunteers and Board of Trustee members may receive confidential or sensitive information relating to Age UK groups or other organisations. The same standards of confidentiality should be adhered to as is the case with clients' information being dealt with at Age UK Sutton.

17.2 Confidential information appertaining to any aspect of Age UK Sutton's work or policies should not normally be sent by fax, however if it is necessary to do so, the first page should clearly indicate that the material is confidential and who should receive it. Prior arrangements should be made with the recipient to ensure that confidentiality is not breached. Mail marked as private and confidential should only be opened by the CEO or board member

17.3 Trustee papers should be stored in a locked filing cabinet marked confidential.

17.4 It is important that care should be taken when using the telephone. The 'hold' facility should be used whenever a conversation with a service user needs to be interrupted. It should also be remembered that no personal caller should be able to hear (witness) a conversation with another service user.

17.4.1 Where two or more conversations are simultaneously taking place on telephones, staff/volunteers should be aware of the nature of these and ensure that confidentiality is not breached.

17.4.2 When calling a person back staff/volunteers should check that the person they want is the person they are speaking to before saying they are from Age UK Sutton.

17.5 Any confidential or sensitive matters appertaining to any aspect of Age UK Sutton work, its staff, volunteers or Board of Trustees, should not in any circumstances be discussed with any third party outside the organisation, without prior authorisation from the CEO. Nor should such information be discussed with a third party within the organisation without prior consultation with the person it concerns or the CEO, whichever would be the most appropriate, depending on the nature of the information (e.g. personal or organisational).

18. Board of Trustees responsibilities

18.1 Board of Trustee members will be expected to respect and adhere to the **Confidentiality Policy** at all times.

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

18.3 Where there may be a conflict with a declared interest of a member of the Board of Trustees, some matters will remain confidential and the procedure at meetings may therefore exclude individuals who 'have an interest'. Trustees who become aware during the course of a meeting that a conflict of interest applies, must declare it immediately.