# Policy 09: Confidentiality

**Last updated by:** SH, RS

**Links to policies:** 12

<table>
<thead>
<tr>
<th>Version</th>
<th>Changes</th>
<th>Policy Date</th>
<th>Next Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>May 18</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Aug 19</td>
<td>Aug 21</td>
</tr>
</tbody>
</table>
1. Introduction

a) Confidentiality is an essential feature of the work of Age UK York (AUKY);

b) AUKY and its Board of Trustees (the Trustees) seek to provide optimum quality services to their service users, their own workers and others with whom they are associated and recognise that high quality services and satisfaction require certainty that personal information is maintained confidentially and treated with respect;

c) AUKY and its Trustees have created and agreed a Data Protection Policy, Policy 12, regarding data protection as an essential feature of confidentiality;

d) Consequently, the Data Protection Policy and this policy, the Confidentiality Policy, are closely linked and should be read together and the requirements and practices of each policy should be taken together.

2. Legislation

a) AUKY and the Trustees acknowledge and adhere to all relevant legislation including the Data Protection Act, 1988 and the General Principles of Data Protection, (GDPR), introduced in 2018;

b) Fuller details of the Data Protection Act and GDPR as they relate to AUKY are set out in Policy 12;

c) AUKY and the Trustees note the existence of civil and criminal offences created by the Data Protection Act, 1988 and ensure that all workers are alerted to these offences at their first Induction session before commencing any role within AUKY;

d) New legislation is introduced from time to time and existing legislation can be updated. The Chief Officer (CO) and Data Protection Working Group (DPWG) regularly review guidance and changes in legislation requirements.

3. Definitions

a) 'Confidentiality' can be defined as the trust that exists between individuals and groups that personal information is not shared except with the knowledge and express permission of such individuals;

b) This information, in the context of AUKY service provision, is quite often held in the mind or memory of the worker or other individual, but may also exist in printed, hand-written, IT based, electronic files, photographs, external memory sticks, hard drives, CD ROMs, video, cloud storage and web/media means;

c) It follows that all workers, on all occasions, will take extreme care to safeguard and not pass on personal information, either orally or by any other means;

d) It is not sufficient for any worker to think only in terms of what is 'commonsense' about not passing on information, but must always bear in mind the terms of this policy, the Data Protection Policy (Policy 12) and the Dignity Policy, (Policy 24);

e) Further information is set out in Policy 12;

f) In any case of doubt, workers should consult their line manager or supervisor and should not discuss any concern they may have with any other colleague.

4. Responsibilities

a) Overall responsibility for adherence to the Data Protection Act, 1988 and GDPR rests with the Trustees, who have devolved day to day responsibility on the CO;
b) The Data Protection Working Group (DPWG), an ad hoc working group consisting of the Chair, CO, Deputy Chief Officer (DCO), Database and Information Officer and Insurance Supervisor, will meet from time to time as required;

c) All AUKY Trustees and workers are responsible for their own actions as regards confidentiality;

d) Workers breaching confidentiality may face disciplinary action.

5. Principles

a) AUKY will:

- respect the confidentiality of all their service users, workers and others with whom they are in contact as a result of their services;
- respect the sensitivity of their service users;
- seek to safeguard the safety and security of their service users and in any situations where that safety and security appear to be jeopardised, will be guided by s.36 of the Data Protection Act, 1988 (exemption from the data protection principles for the purposes of an individual's personal, family or household affairs);

b) AUKY will take due care in the collection and storage of data and will do their utmost to keep all data accurate, timely and secure;

c) Much information about service users and others may be known to AUKY workers and not recorded. Confidentiality will be maintained even where data are not recorded so as to fall within the terms of the Data Protection Act, 1988.

6. Training

a) All AUKY Trustees and workers will be given training regarding confidentiality at their first induction session. They will be:

- informed about who should have access to personal/sensitive information;
- helped to understand their obligations about confidentiality and sensitivity;
- helped to understand how the security measures that AUKY implements are appropriate;
- advised always to seek guidance from their line manager or supervisor in all cases of doubt;

b) Workers will be helped to arrive at a clear understanding of practice and expectation within AUKY. This will include:

- with whom it is appropriate to share information;
- guarding against unauthorised access to or alteration, disclosure, or destruction of personal data;
- accidental loss or destruction of personal data;
- dealing with general public enquiries;
- establishing the identity and entitlement of any person making enquiries before disclosing any information;
- actions to be taken if doubts or concerns arise;
- never discussing or disclosing sensitive information to anyone without first ascertaining that they are an appropriate person to share and the client has given consent;
- a duty of candour;

c) While taking care to protect the confidentiality of service users, workers will also be advised at Induction:
• Not to disclose their own personal information to service users;
• Not to give service users or others their personal phone numbers or any other worker's phone numbers;
• To use 141 before making any call from a land line or a mobile.

7. Complaints

a) The DPWG will advise the CO regarding complaints about confidentiality;

b) Complaints breaches of confidentiality will be dealt with as follows:
   • Workers who are dissatisfied with any arrangements regarding confidentiality or the protection of their personal data should use AUKY’s Grievance Policy;
   • Service users who are dissatisfied with any arrangements regarding confidentiality or the protection of their personal data should raise their concerns with their service-providing worker or that worker's line manager or supervisor. Service users may contact the CO direct if necessary or use the Complaints Policy;
   • All complaints will be dealt with as quickly and responsively as possible. In terms of the Data Protection Act, 1988, any complaint received that questions AUKY’s policy and/or procedure will be dealt with immediately;

c) The DPWG will take particular notice of the requirements of the Grievance Policy regarding involvement of Trustees in investigation of a complaint;

d) In keeping with the data protection and confidentiality principles, workers should not discuss their concerns other than with their line manager, supervisor or CO except as set out in the Grievance Policy;

e) The DPWG will be informed of all correspondence and other developments that may occur during the course of the complaints process;

f) A repository of all AUKY statements of Data Protection Law compliance and information about any contacts made will be maintained by the Data Protection Controller. This information will be available to staff and others on whom data are held, on request.