Policy 12: Data Protection

Last updated by: SH, RH

Links to policies: 9

<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>Nov 18</td>
<td>Sep 19</td>
</tr>
</tbody>
</table>
1. Introduction and Purpose

This policy:

i) Applies to Age UK York (AUKY);

ii) Is directly associated with Policy 9, the Confidentiality Policy and should be read alongside it;

iii) Details the duties of all AUKY workers regarding the Data Protection Act 2018, General Data Protection Regulations and Record Retention procedures;

iv) Sets out the standards expected of all AUKY workers in relation to record retention and disposal of personal and sensitive data and the safeguarding of individual's rights within AUKY;

v) Explains the rules relating to data breach and subject access requests and provides definitions;

vi) Provides, via the website, a Privacy Notice that is made available to all service users, explaining how their data are used and their right to complain about any suspected breach;

vii) Provides, via the website, a similar Privacy Notice for all AUKY workers.

2. Scope

This policy covers all records held by Age UK York irrespective of the media on which they are created or held, including oral, printed, hand-written, IT based, electronic files, photographs, external memory sticks, hard drives, CD ROMs, video, cloud storage and web/media.

3. Legislation

i) AUKY acknowledges and works within the Data Protection Act, 2018 and the General Data Protection Regulations (GDPR);

ii) The Chief Officer (CO) is the Data Controller, also known as the Data Protection Controller, in accordance with the legislation and is registered with the Information Commissioner;

iii) The Data Protection Act, 2018, has created responsibilities relevant to AUKY regarding the storage, processing and transmitting of data, and the rights of its service users and others about whom such data are collected;

iv) The general principles of the Data Protection Act, 2018 are that data must be:
   • obtained and processed fairly and lawfully;
   • held only for special purposes;
   • adequate, relevant and not excessive;
   • accurate and up to date;
   • not kept longer than necessary;
   • processed in accordance with the Act;
   • kept secure and protected;
   • not transferred elsewhere without adequate protection;

v) The Caldicott Review and the second review, termed Caldicott2 Review, had set out, in 2016, 7 Principles for the guidance of data protection interpretation. These Principles are:
   • Justification of the purpose(s) for disclosing confidential information. Every instance must be considered individually;
   • Patient identifiable data must not be used unless absolutely necessary and where there are no alternatives. [AUKY notes that referring to patient identifiable information when commissioning care for patients with unique health conditions or repatriating patients to home based services is a
particular danger for data breach in the context of the services that AUKY provides to its service users.]

- Where data are disclosed, the minimum amount necessary should be transferred, taking into account the purpose for which those data are required. [AUKY notes that its workers will tend to have a range of knowledge or understanding of particular service users. Such knowledge or understanding may be passed on in general conversation at a disclosure point. Workers must beware of such behaviour and be able to justify passing on such knowledge in each instance.];

- Access to patient identifiable information should be on a strictly need to know basis. Only those individuals who need to see patient identifiable information should have access to it and they should only have access to the information they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes. The disclosure of patient identifiable information will very often be a question of balance and one consideration will be the question of any harm or prejudice caused to the patient if the information were to be disclosed;

- Everyone with access to patient identifiable information must be aware of their responsibilities. [AUKY notes that it is the duty of supervisors, before any worker has access to any service user records, that they receive training in the appropriate handling of service user information and of essential practices in safeguarding service user confidentiality.];

- Understanding of and compliance with the Data Protection Act, 2018 and with any amendments is essential in the context of data protection and confidentiality;

- The duty to share information can be as important as the duty to protect patient confidentiality. [AUKY notes that the sharing of information must be in the best interests of service users. Further information is contained within this Policy and in any case of doubt, workers must immediately contact their line manager or supervisor.]

vi) Under the Data Protection Act, 2018, several criminal and civil offences exist:

- It is an offence to process personal information without registration;
- It is an offence for either or both AUKY or a worker to use personal information for a purpose other than that registered;
- It is an offence for people such as hackers and impersonators, outside AUKY, to obtain unauthorised access to personal data;
- It is a criminal offence to request information about an individual relating to cautions or convictions for the purposes of recruitment, continued employment, or the provision of services;

vii) AUKY has a legal duty to disclose certain information including information about actual or suspected abuse of vulnerable adults to social services or the police; where the law requires or, for example, to its auditors to enable a satisfactory audit of its affairs;

viii) In any instance where a breach of confidentiality or of the Data Protection Act, 2018, appears to have occurred, workers will first discuss the matter with their line manager, supervisor or CO but with no one else;

ix) In any situation where there appears to be a conflict of interest, for example between a service user and carer, workers must discuss the situation with their line manager or supervisor or the CO but with no one else;

x) New legislation is introduced from time to time and existing legislation can be updated. The CO and DPWG regularly review guidance and changes in legislation requirements.

3 Policy 12: Data Protection v2
4. Responsibilities

i) Overall responsibility for adherence to the Data Protection Act, 1988 rests with the Trustees of AUKY, who have devolved day to day responsibility on the CO;

ii) The Data Protection Working Group (DPWG), an ad hoc working group consisting of the Chair, CO, Deputy Chief Officer (DCO), Information Officer and Insurance Supervisor, will meet from time to time as required;

iii) All AUKY Trustees and workers are responsible for their own actions as regards accurate collection, data handling and confidentiality including the maintenance of accurate organisational data systems;

iv) All AUKY Trustees and workers have a responsibility to protect the integrity and confidentiality of all personal data held with regard to its service users and workers;

v) Workers accessing unauthorised files or breaching confidentiality may face disciplinary action. Ex-staff breaching confidentiality may face legal action;

vi) All AUKY Trustees and workers will be given training regarding data handling and 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.

vii) 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.

5. Complaints

i) The DPWG will advise the CO regarding complaints about confidentiality, possible breaches of the Data Protection Act, 1988 or for any other reason regarding data protection;

ii) Complaints about data protection and 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.
iii) Records of all correspondence will be kept for five years;

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

v) 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;

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

vii) All records of Data Protection complaints relating to AUKY will be kept in the Finance and Administrative Office in the Walmsgate AUKY building, along with its organisational complaints policy and paperwork records;

viii) 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.

6. Principles
i) 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, 2018 (exemption from the data protection principles for the purposes of an individual’s personal, family or household affairs);

ii) 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;

iii) Normally, only data relevant to the services of AUKY will be collected and processed;

iv) 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, 2018;

v) Any individual in contact with AUKY has the right to assume that all information that might be construed as sensitive will be treated in confidence and not passed on without their specific consent. That consent will be in writing or printable form;

vi) The principle of confidentiality applies to information about all the internal affairs of AUKY;

vii) Workers will not discuss information that is the subject of investigation for confidentiality with anyone else, including within AUKY, except as authorised by the CO.

7. Definitions
i) “Personal data” covers any data that can be used to identify a living individual. An individual is entitled:
   • to be informed whether personal data are held of which they are the subject;
   • to access any such data, for which they may make a Subject Access Request via www.ico.org.uk or the ICO helpline 0303 123 1113;
   • when appropriate, to have such data corrected or erased.
ii) “Data” means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose and includes computer-generated material;

iii) Any data file or record which contains personal data of any form can be considered as confidential in nature;

iv) Anonymised or aggregated data are not regulated by the Act, providing the anonymisation or aggregation has not been done in a reversible way;

v) Individuals can be identified by various means including their name and address, telephone number, e-mail address or via social media;

vi) The Act applies only to data which are held, or intended to be held, via some mechanical or electronic means or in a filing system including paper systems such as a service provider's notebook or diary;

vii) 'Sensitive' includes what is covered in definitions of discrimination, racial or ethnic origin, political opinions, religious beliefs, physical or mental health, marital status, sexual life and civil or criminal offences, as well as information relating to actual or potential disputes and actual or potential commercial or contractual agreements;

viii) This principle does not apply where information is already in the public arena such as in annual reports, statements of accounts and directories;

ix) In any case of doubt regarding confidentiality of a service user's details, the CO will make a decision, taking into account the service user's own Letter of Agreement (see Policy 51);

x) The DPWG will consider what data can be held regarding views, comments, identification of unmet need and anything else that will monitor and enhance the quality of service provided, that can be collected in anonymised, aggregated and irreversible ways, thereby not falling within the requirements of the Data Protection Act, 2018;

xi) The DPWG will similarly consider what data can be held regarding the profiles of service users and workers that can be anonymised, aggregated and rendered irreversible.

8. Related Policies

i) AUKY adheres to the multi-agency policy ‘No secrets’ for the protection of vulnerable adults;

ii) All AUKY workers will ensure they follow the requirements of the Data Protection Act, 2018 and take particular note of how this Act relates to their own areas of work, for which a specific policy may also exist;

iii) In any case of doubt, workers will discuss the situation with their own line manager or supervisor.

9. Passwords and General Security of Data

i) AUKY undertakes appropriate 'Safer Recruitment' practices relevant for employees who have access to service user data and undertakes similar care in the case of volunteers;

ii) AUKY is responsible for ensuring that the records and systems are backed up on a regular basis and that there is no loss or destruction of personal data accidentally. If workers are aware of any errors or have any concerns regarding personal data this should be reported immediately to their line manager or supervisor;

iii) Information about password use is to be found throughout this Policy and must be followed;

iv) Workers must not give out passwords to others who may then acquire access to data they are not entitled to view;
v) Although re-use of paper is good environmental practice, workers must not re-use (the backs of) reports that contain personal data but should arrange for their immediate shredding;

vi) Where workers take out of AUKY's own venues laptops or other digital devices capable of holding confidential information, or paper files etc, they are required to take particular care to keep all such devices safe and, if appropriate, in locked vehicles. Access to any laptops used in this way must be passworded;

vii) All data, however kept, will be stored securely. This may involve the use of lockable key cabinets and/or computer protection systems about which AUKY may take advice from their computer systems provider.

10. Data Collection

i) At the first contact with a service user, the AUKY service provider/worker will:

- Provide and discuss the privacy Notice (Appendix 1);
- Discuss aspects of storage and sharing information with the service user;
- Ensure they understand what information will be shared and who it will be shared with;
- Use the standard format to show this information and have it signed by the service user/carer/relative;
- Always bear in mind the ‘Best interests’ of the service user;
- Ensure that the service user is kept informed of changes in the future;

ii) Having regard to the requirements of the Data Protection Act, 2018, in the collection of data, all AUKY workers will:

- Only collect data that are obtained and processed fairly and lawfully;
- Only collect data that are adequate, relevant to the carrying out of the legitimate purposes and functions of the charity, not excessive in relation to those purposes and only disclosed to appropriate people;
- Inform those about whom data are collected that these data will be stored at the time of collection;
- Ensure that data are collected only in ways that are not prejudicial to the interests of individuals;
- Use a standard statement for all written requests for data and a similar verbal script for phone data collection. Such statements and scripts will include the phrase ‘in keeping with the Data Protection Act, 2018’;
- Make every effort to ensure the accuracy of data and date all such information;
- Assume that individuals have given their data in accordance with the principles of AUKY and for the promotion of the older people of York;
- Only process that data in line with the relevant individual’s rights;
- Request the express permission of any service user where data are intended to be used for any other reason. In any such instance the data will be rendered into an irreversible format so that individuals cannot be identified;
- Keep the data secure and not keep it for longer than is necessary;
- Not transfer that data to other countries without adequate protection.

11. Handling and Processing of Data

i) All data on individual subjects will be treated in a consistent way. Subjects will be informed about how AUKY will store and use the data at the time of collection;

ii) All appropriate data processing will be included in existing AUKY databases and subsequently in the organisational databases;

iii) In accordance with the Environmental Policy, workers should seek to make as little use of paper as possible and should record as much information as possible in digital formats;

7 Policy 12: Data Protection v2
iv) Any data processing will only be allowed where there is a clear rationale for the activity which meets the Data Protection Act, 2018, criteria;

v) All manual files and electronically-held data will be kept up to date;

vi) Any agent employed or volunteering to process data on AUKY’s behalf will be bound by a written contract to comply with AUKY’s data protection policy;

vii) Workers will receive specific guidance from their line manager or supervisor when taking data from the office. This guidance will include:

- security awareness;
- back up processes and security of external providers;
- transportation of electronic data e.g. memory sticks, external hard drives and mobile phones;
- email management.

12. Storage of Data
i) Data may be stored in a variety of ways such as in manual files or various electronic means;

ii) AUKY is moving onto Charitylog, a program for secure storage of data. All staff are in process of being trained for use of Charitylog. In any case of doubt as to its use, staff should consult their line manager or supervisor;

iii) All data and records will be stored as securely as possible, reflecting the sensitivity and confidential nature of this material, in order to avoid potential misuse or loss;

iv) Sensitive data will only be kept at AUKY’s main office at Walmgate or its 'annex' at the Priory Street Centre, unless agreed by the DPWG. Paragraph 13 iii) is also relevant;

v) Non-sensitive data may be stored elsewhere having regard to convenience, the period of retention required and the frequency with which the records may need to be accessed. The DPWG will review these arrangements from time to time;

vi) All data held by electronic means will be password protected as arranged by the Data Controller;

vii) Large quantities of data may be archived by methods which are as equally secure as current data. Archived data will be organised so as to permit ease of access and retrievability;

viii) An archiving policy will be created by the DPWG and CO and a clear rationale will be supplied for personal data to be kept beyond five years;

x) The Data Controller in discussion with the DPWG may in future create and put in place arrangements regarding the use of laptops including how much information is actually held on any laptop and how much is only kept on USB devices kept at AUKY’s own venues;

xi) When the new AUKY database is in use all workers will be trained in the use of the system. Only named appropriate workers will have access to subject data.

13. Data use for non-AUKY Services
i) Personal data will only be processed fairly and lawfully. In order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data:

- The person whose data is stored has given their permission to the processing;
- Processing is necessary for the performance of, or commencing, a service;
- Processing is required under a legal obligation;
• Processing is necessary to protect the vital interests of the person to whom the data relate;
• Processing is necessary to carry out any public functions;
• Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).

ii) Where data are passed to a third party, AUKY will ensure that a written contract is put in place that states that the third party will work within AUKY’s data protection policy;

iii) AUKY will inform individuals of any processing or disclosure that does not fall within AUKY’s purpose in a way that any individual supplying could be expected to understand. AUKY will keep such notification up to date.

14. Access to Data

i) AUKY will keep files of all its workers, recording details such as gender, disability, age, employment and sickness records together with contact details. These will be kept in secure cabinets. Any worker has a right to see their own file at any convenient time on request. Only those records will be kept that relate to any worker’s employment or role;

ii) Service users are entitled to have access to and examine any data about them that are held by AUKY. Workers will assist service users to access and understand any such data;

iii) Where information is requested by service users and workers, workers will:
  • make every effort to ensure that immediate action is taken when a data access is requested;
  • Send a standard letter (amended as appropriate) to the individual stating AUKY policy on subject access. This will promise to provide the required data to the best of AUKY’s ability within 40 days;
  • Search to ensure that all relevant data are collected. The search will include all electronic data and manual files. Information on data collection, storage, processing and transfer may be supplied to the individual;
  • Collate the requested information in printed format for which a charge may be made; but this charge will not be made unreasonably;
  • Offer the information to the individual at AUKY’s premises with a member of paid staff on hand to help with any queries or interpretations. If the individual is unable to visit AUKY premises, alternative arrangements can be negotiated.

15. Disclosure of Data

i) Any requests for details of personal data held by AUKY should immediately be sent to the Data Protection Controller, (the CO) who will deal with the request or will authorise employees to do so;

ii) Failure to comply with this requirement could be treated as misconduct;

iii) Unauthorised disclosure of data whether in oral, printed, hand-written, IT based, electronic files, photographs, external memory sticks, hard drives, CD ROMs, Video, cloud storage, web/media must be avoided;

iv) Where sensitive data are involved, workers should not disclose data to outside agents except in cases agreed by the DPWG;

v) Worker's home contact details will not be given to any service user, other organisation or member of the public without that worker's express permission each occasion it is requested;

vi) No data of any kind will be released for the purpose of direct marketing;

9 Policy 12: Data Protection v2
vii) AUKY will not allow data collected from individuals to be disclosed to third parties except in circumstances which meet the requirements of the Data Protection Act. These are:

- the individual has been informed of this use of their data, has consented to their disclosure and, unless there is a legal obligation for that disclosure, has been offered the chance to opt out;
- AUKY is legally obliged to disclose the data;
- there is a business requirement to disclose data that are within the remit of the Data Protection Act and are not prejudicial to the interests of the individual.

viii) Before any new disclosure is made the data must be checked for suitability by the DPWG. Any request for data based on a legal requirement e.g. from the police or other body, must be in writing and checked against advice of the Data Protection Registrar. In all cases of doubt, the DPWG should seek advice from the Data Protection Registrar;

ix) All workers will ensure that any general disclosure is recorded on a record of disclosures held by the Data Controller. The record will include a clear rationale as to why this disclosure is taking place.

16. Storage and Minimum Retention Period of Data

i) The Data Protection Act 2018, requires that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose;

ii) A record retention schedule is maintained and, taking note of any legislative changes, indicates timescales for which records are to be kept. This schedule falls within the responsibility of the DPWG and CO who derive the recommended times from:

- AUKY’s organisational needs as determined by the DPWG and CO;
- Legislation;
- Care Quality Commission.

iii) Accessible, accurate and well organised historical records and documentation are an effective way of addressing any disputes or investigations;

iv) Changes within the employment and pension legislation make the need to retain some aspects of employee information for much longer than was previously the case. Government guidance, via its website, advises that such information is kept past retirement.

17. Disposal and Destruction of Data

i) Data about any individual remain confidential and subject to the Data Protection Act, 2018 throughout the time they are held by AUKY whether ‘live’ or archived;

ii) To ensure compliance with the Data Protection Act 2018, all information, in any format, destroyed from any AUKY location must not expose confidentiality of its workers, service users and customers;

iii) Where data are brought up to date, if the old data are kept on paper, that paper will be shredded. On all occasions if data are transferred from paper to digital format, the paper will be immediately shredded. If kept electronically data will be regarded as destroyed once over-written. The DPWG may take advice on this from its computer systems supplier;

iv) The decision on disposal of data and retention period rests with the Data Controller and DPWG. They will take into account:

- On-going business and accountability needs (including audit);
- Current applicable legislation;
• Whether the record has any long term historical or research value;
• Best practice in the applicable field;
• Costs associated with continued storage versus costs of destruction;
• The legal, political and reputational risks associated with keeping, destroying or losing control over the records;
• Whether the data be returned to the sender/provider to be stored e.g. NHS or CYC.

v) The decision to destroy should not be made with the intent of denying access or destroying evidence;

vi) Where appropriate, a review should be conducted with stakeholders including the AUKY legal adviser, external bodies e.g. CQC, and contract funders;

vii) An AUKY officer is tasked with maintaining a system of documentation for confirmation of destruction to enable employees to know what has been archived and what has been destroyed. This is managed by the officer overseeing the management and maintenance of the organisational database. S/he works under the guidance of the Data Controller and the DPWG. This documentation includes:

• Description of the data/record;
• Type of data (paper, IT);
• Creation date of record, review and decision date;
• Disposal decision and method of disposal;
• Summary of reasons for decision;
• Names of people involved in decision;
• Signature of person authorising disposal.

vii) Personal data will not be held for longer than necessary and when such data are earmarked for destruction, appropriate measures will be taken to ensure that the data cannot be reconstructed and processed by third parties;

viii) Data may only be kept about living individuals. However, for historical reasons the CO is executor for some service users. In such instances it may be necessary for the CO to continue to hold data after the death of any such individual. Such data will be destroyed by confidential means as soon as possible;

ix) The Data Controller will ensure that shredded paper is collected in secure ways. AUKY has engaged a private business to undertake the destruction of confidential waste. This is organised and arranged by Jan Hunter and Rebecca Hall at the Walmgate Office;

x) All other paper is disposed of in the boxes or bins provided in workers’ offices;

xi) The Data Controller will, from time to time, review confidential data including those held about AUKY themselves and arrange for their deletion;

xii) The Data Controller may, with the DPWG, create a policy regarding the length of time of holding data. This policy, the Archives Policy, is numbered 49;

xiii) Financial data must be kept for seven years regardless of format;

xiv) The destruction of confidential or sensitive waste on electronic media such as memory sticks/CD/external hard drives/laptops tape, disk, cassette/cartridge, hard drives, CD-ROMs, DVD and
ZIP drive is undertaken under the guidance of AUKY's IT support organisation Mansys. Destruction of back-up copies of such data is dealt with in the same manner.

18. Workers Leaving AUKY

i) 'Workers' includes all paid staff, volunteers and Trustees of AUKY and, for the purposes of the requirements of the Data Protection Act, 2018 includes anyone on placement, secondment or training;

ii) On leaving AUKY all workers will hand over any ID cards which will then be destroyed. Workers will also hand over any keys to data cabinets, any laptops or mobile phones belonging to AUKY and will reveal all passwords;

iii) It is not desirable that workers use any laptop or mobile phone of their own for work purposes. However, if such use is made in emergency, they will discuss this fact with their line manager or supervisor and will ensure that no confidential data remains on such equipment, whether they leave AUKY or not;

iv) The Data Controller will decide whether to change all passwords following the departure of a worker and in any event will have instituted procedures so that all passwords are changed from time to time.