Document Name:	**Data Protection Policy**
Approved by Board of Trustees on:	06 September 2018
Review Schedule	Every two years
Next review due	September 2020 Cfwd to Apr 2021
Owner (Responsibility)	Chief Executive Officer

Document Description:

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how Age UK Wiltshire meets them.

Implementation & Quality Assurance

Implementation is immediate, and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every two years by the Board of Trustees, or sooner if legislation, best practice or other circumstances indicate this is necessary. All aspects of this Policy shall be open to review at any time.

Revision History

Revision date	Summary of Changes	Other Comments
27 Aug 2019	Updated Section 9 Cloud Computing (9.5, 9.6, 9.7 9.8) references to data processors	EP
14 Jan 2020	Updated policy to include direct marketing changes (section 6). Sections reordered.	EP/JT

Glossary of Terms

AUKW – Age UK Wiltshire

Board – Board of Trustees, the collective term for all Trustees (see below)

Casual Workers – the paid personnel of the charity with a Terms of Engagement rather than a contract of employment, their terms and conditions differ from those of employees; distinct from employees

CEO – Chief Executive Officer, the most senior paid employee within the charity, accountable to the Board of Trustees

the Charity – Age UK Wiltshire

CharityLog – the database used to record & store details of AUKW clients, staff, volunteers, Trustees and other contacts

Client – an individual in receipt of support from one or more of AUKW services

DBS – Disclosure and Barring Service; used to refer to the check made on an individual to ensure they are suitable to work with vulnerable individuals

Employees – the paid personnel of the charity with a Contract of Employment, whether that be permanent, temporary or fixed term; distinct from Casual Workers

FRSC – Finance and Resources Sub Committee – a sub-committee of the Board

GSC – Governance Sub Committee – a sub-committee of the Board

Leadership Team (LT) – comprises the members of the SLT PLUS the Area Manager, Programmes Manager and Fundraising and Partnerships Manager

Senior Leadership Team (SLT) – comprises the CEO, Director of Services, Director of Paid for Services and Finance Manager

Staff – collective term for all paid personnel within the charity irrespective of their contract type; includes both employees and casual workers

Trustees - The people who share ultimate responsibility for governing the charity and directing how it is managed and run. The Trustees are legally responsible for the charity. Trustees are volunteers and are not paid other than reimbursement of expenses.

Volunteers – the unpaid personnel of the charity, volunteers give their time freely and are not obliged to do work for the charity, equally the charity is not obliged to provide them with work, volunteers do not have rights under employment law

1. Introduction

1.1. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR applies from 25 May 2018.

1.2. The following guidance is not a definitive statement on the Regulations but seeks to interpret relevant points where they affect Age UK Wiltshire.

1.3. The Regulations cover both written and computerised information and the individual's right to see such records.

1.4. It is important to note that the Regulations also cover records relating to staff and volunteers.

1.5. All Age UK Wiltshire staff are required to follow this Data Protection Policy at all times.

1.6. The Chief Executive Officer has overall responsibility for data protection within Age UK Wiltshire, but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

2. Definitions

2.1. **Processing of information** – how information is held and managed.

2.2. **Information Commissioner** - formerly known as the Data Protection Commissioner.

2.3. **Notification** – formerly known as Registration.

2.4. **Data Subject** – used to denote an individual about whom data is held.

2.5. **Data Controller** – used to denote the entity with overall responsibility for data collection and management. Age UK Wiltshire is the Data Controller for the purposes of the Act.

2.6. **Data Processor** – an individual handling or processing data

2.7. **Personal data** – any information which enables a person to be identified

2.8. **Special categories of personal data** – information under the Regulations which requires the individual's explicit consent for it to be held by the Charity.

3. Data Protection Principles

3.1. As Data Controller, Age UK Wiltshire is required to comply with the principles of good information handling.

3.2. These principles require the Data Controller to:

- process personal data fairly, lawfully and in a transparent manner;
- obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained;
- ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held;
- ensure that personal data is accurate and, where necessary, kept up-to-date;
- ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained;
- ensure that personal data is kept secure;
- ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

4. Consent

4.1. Age UK Wiltshire must record service users' explicit consent to storing certain information, known as 'personal data' or 'special categories of personal data', on file.

4.2. For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

- the racial or ethnic origin of the data subject;
- his/her political opinions;
- his/her religious beliefs or other beliefs of a similar nature;
- whether he/she is a member of a trade union;
- his/her physical or mental health or condition;
- his/her sexual life;
- the commission or alleged commission by him/her of any offence;
- online identifiers such as an IP address;
- name and contact details;
- genetic and/or biometric data which can be used to identify an individual.

4.3. Special categories of personal information collected by Age UK Wiltshire will, in the main, relate to service users' physical and mental health. Data is also collected on ethnicity and held confidentially for statistical purposes.

4.4. Consent is not required to store information that is not classed as personal or special categories of personal information, as long as only accurate data that is necessary for a service to be provided is recorded.

4.5. As a general rule, Age UK Wiltshire will always seek consent where personal or special categories of personal information is to be held.

4.6. It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

4.7. If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Services Manager or Chief Executive Officer for advice.

5. Obtaining Consent

5.1. Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face;
- written;
- telephone;
- email.

5.2. For face-to-face or written consent, pro-forma should be used. It should be specific and 'granular' so that separate consent is obtained for separate things. Each consent statement should give the person an opportunity to make an affirmative choice to agree. Tick boxes can be used but not pre-ticked boxes or any other method of default consent.

5.3. For telephone consent, verbal consent should be sought and noted on the case record.

5.4. A standard consent script will be used when communicating with clients. This standard script is given below. Variations of the standard script may exist for individual services where the standard script is not appropriate.

5.5. Standard Consent Script:

Using and storing your data

"Everything you tell us is treated confidentially. We will securely record your personal data, which may include health, gender and ethnicity, and we share this with our partner organisations in order to deliver our services. We may write to you with information about our services and activities if we think this could be of interest. We will not pass on or sell your details for marketing purposes. Is this okay?"

Evaluating the service, we have provided you with
"Evaluations and feedback are really helpful and mean we can develop and improve our services. These are carried out by us and our project partners. Would you like to participate in these?"
"The information we record is occasionally looked at by Age UK auditors, to assess the quality of our services. Is this ok?"

Talking to others on your behalf
"Would you like to give permission for another person/organisation to speak to us on your behalf about your situation? We may share personal and sensitive information with this person."
"Thank you for providing this information; if you change your mind you can amend or withdraw your consent preferences at any time."

Keeping in touch by email (where appropriate)
"We'd like to email you occasionally with details of the work we do for older people and opportunities to support us. Is this okay?"

5.6. For e-mail consent, the initial response should seek consent as below.

5.7. Standard Consent Script:

Using and storing your data
"Everything you tell us is treated confidentially. We will securely record your personal data, which may include health, gender and ethnicity, and we share this with our partner organisations in order to deliver our services. We may write to you with information about our services and activities if we think this could be of interest. We will not pass on or sell your details for marketing purposes. Is this okay?"

5.8. Consent obtained for one purpose cannot automatically be applied to all uses, e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of products were to be undertaken.

5.9. Preliminary verbal consent should be sought at the point of initial contact, as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record such as CharityLog. The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by Age UK Wiltshire, then the Service Co-ordinator should discuss with the Services Manager at the earliest opportunity.

6. Direct Marketing

6.1. The information Commissioner's Office (ICO) defines Direct Marketing in section 122(5) of the Data Protection Act 2018 as:
"the communication (by whatever means) of advertising or marketing material

which is directed to particular individuals"

For Age UK Wiltshire this means that any communication sent to individuals about fundraising, services, news, updates or the Aims and Objectives is classed as direct marketing.

6.2. Age UK Wiltshire will undertake direct marketing to promote the services offered, the work undertaken, events, campaigns and fundraising opportunities.

6.3. For direct marketing purposes, Age UK Wiltshire may store and use marketing information for:

- its workforce, including trustees, staff, and volunteers;
- its beneficiaries, including clients, groups and other organisations;
- its supporters, including donors, members and funders.

6.4. In order to send direct marketing materials, Age UK Wiltshire will either seek specific consent by a preferred communication method or will use Legitimate Interests where it can be demonstrated that this would have a minimal privacy impact and the person would reasonably expect to receive it. Direct marketing materials will not be sent by a particular communication method if Age UK Wiltshire has been told that information should not be sent in this way.

6.5. Before marketing materials are sent under a Legitimate Interest, a Legitimate Interest Assessment will be undertaken to show that Age UK Wiltshire has considered the three tests; purpose, necessity and balance. A record will be kept for the justification of the Legitimate Interest.

6.6. Age UK Wiltshire will not share or sell its database(s) with external organisations for marketing purposes.

6.7. It is recognised that people, groups or organisations for whom records are held have the right to change their minds about what information is sent to them and how they receive it.

7. Ensuring the Security of Personal Information

7.1. Unlawful disclosure of personal information

- It is an offence to disclose personal information 'knowingly and recklessly' to third parties.
- It is a condition of receiving a service that all service users for whom personal details are held, should provide consent allowing Age UK Wiltshire to hold such information.
- Service users may also consent for Age UK Wiltshire to share personal or special categories of personal information with other helping agencies on a need to know basis.
- A client's individual consent to share information should always be checked before disclosing personal information to another agency.

- Where such consent does not exist, information may only be disclosed if it is in connection with criminal proceedings, or in order to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive Officer or Services Manager should first be sought.
- Personal information should only be communicated within Age UK Wiltshire's staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

8. Use of Files, Books and Paper Records

8.1. In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records will be kept in locked cabinets and drawers overnight, and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working day.

9. Disposal of Scrap Paper, Printing or Photocopying Overruns

9.1. Names, addresses, phone numbers and other information written on scrap paper are also considered to be confidential.

9.2. If transferring papers from home, to a client's home, or to the office for shredding, this should be done as soon as possible and avoid leaving documents in a car for any period of time. When transporting documents, they should be carried out of sight.

10. Computers

10.1. Access to personal and special categories of personal information is restricted by password and restricted access control to authorised personnel only.

10.2. Computer monitors in the reception area, or other public areas, must be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible, then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, e.g. reception, computers will be locked when left unattended.

10.3. Documents should only be stored on the server or cloud-based systems and not on individual computers.

10.4. Where computers or other mobile devices are taken for use off the premises the device will be password protected.

10.5. Cloud Computing

10.5.1. When commissioning cloud-based systems, Age UK Wiltshire will satisfy itself as to the compliance of data protection principles and robustness of the cloud-based providers.

10.5.2. Age UK Wiltshire currently uses three cloud-based data management systems to hold and manage information about its service users and donors/supporters.

10.6. Charitylog (Dizions)

10.6.1. Charitylog, hosted by Dizions Ltd, holds data about staff, volunteers and clients. Access is password protected and restricted to named users, with level of access to each user on a 'need to know' basis to be able to carry out their job. Charitylog is accredited to ISO 27001:2013 Information Security standard. It is also accredited to the International Quality Management Standard ISO 9001:2015 and registered with the Information Commissioners Office. Age UK Wiltshire is satisfied with the security levels in place to protect its data.

10.7. HostingIT4U

10.7.1. Age UK Wiltshire have satisfied themselves that the security levels in place to protect its data are suitable and that HostingIT4U are using data centre's (Access Alto) that have accredited to ISO 27001:2013 Information Security standard and also ISO 9001:2015 International Quality Management Standard.

10.8. Quickbooks (Intuit)

10.8.1. Age UK Wiltshire have satisfied themselves that Intuit, (owners and providers of Quickbooks), have signed up to the EU-US Privacy Shield self-certification program which is approved by the ICO as being compatible with UK data protection regulations.

11. Privacy Statements

11.1. Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- explain who Age UK Wiltshire is
- what we will do with their data
- who the information will be shared with
- consent for marketing notice
- how long the information will be kept
- that the data will be treated securely
- how to opt out
- where they can find a copy of the full notice.

11.2. A fuller Privacy Policy is published on our website.

12. Personnel Records

12.1. The Regulations apply equally to staff and volunteer records. Age UK Wiltshire may, at times, record special categories of personal data as part of a staff member's contract of employment or with the volunteer's consent.

12.2. For staff and volunteers who support vulnerable adults, it will be necessary for Age UK Wiltshire to apply to the Disclosure and Barring Service (DBS) to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Senior Management Team and authorised members of the Business Support Team. If there is a positive disclosure the Chief Executive Officer will discuss this, anonymously, with the Chair of the Standards Committee and the insurers to assess the risk of appointment. Trustees and insurers should not see the report itself.

13. Confidentiality

13.1. When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for Age UK Wiltshire must not be stored on a private external hard disk or computer. If documents need to be worked on at a non-networked computer, they should be saved to a USB drive which should be password protected.

13.2. Workstations in areas accessible to the public, e.g. reception or trading office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

13.3. Any paperwork kept away from the office, such as a client's care plan kept at home by a worker), should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view, such as on a desktop, but kept in a file in a drawer or filing cabinet. The optimum is a locked cabinet, but safely out of sight is a minimum requirement. Enablers needing to take paperwork away from a client's home, such as unable to make a required phone call during the visit, must ensure that it is returned to the client's home on the next visit.

13.4. If documents are being carried relating to a number of clients when on a series of home visits, the documents for other clients should be kept locked and out of sight in the boot of the car, and not taken into the client's home. When carrying paper files or documents, they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase, folder or bag should contain Age UK Wiltshire's contact details. Only personal data necessary for the job in hand should be taken on a visit. Care should be taken to ensure that the correct number of documents is taken away from a client's home and nothing is left behind.

14. Retention of Records

14.1. Paper records should be retained for the periods set out in the Data Map at the end of which they should be shredded or securely destroyed, in the case of physical records, or deleted in the case of electronic records.

14.1.1. Additional document retention periods are outlined below:

- timesheets and other financial documents – seven years;
- employer's liability insurance – 40 years;
- hirer agreement – six years after the date of the agreement;
- other documentation, such as a client's care plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

14.2. Records that are identified as no longer in active use but are inside the retention period will be archived where possible. Archived records should clearly display the destruction date.

14.3. Computerised records, e.g. documents and CharityLog records, to be deleted or anonymised after the retention period. Anonymising a CharityLog record will remove the personal and special categories of personal data, but will not remove the statistical data.

15. What to do if there is a breach of the Policy:

15.1. If it is discovered, or suspected that data protection has been breached, this should be reported this to a line manager who will review the systems, in conjunction with the Senior Management Team, to prevent a reoccurrence.

15.2. The CEO should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and for reporting to the Board of Trustees.

15.3. Any deliberate or reckless breach of this Data Protection Policy by a member of staff or volunteer may result in disciplinary action, up to and including dismissal.

16. The Rights of an Individual

16.1. Under the Regulations, an individual has the following rights with regard to those who are processing his/her data.

- Personal and special categories of personal data cannot be held without the individual's consent. However, the consequences of not holding it can be explained and a service withheld.
- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - where data is no longer necessary in relation to the purpose for which it was originally collected;
    - when an individual withdraws consent;
    - when an individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
    - personal data was unlawfully processed.
- An individual has a right to restrict processing – where processing is restricted, Age UK Wiltshire is permitted to store the personal data, but not further process it. Age UK Wiltshire can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.
- When Age UK Wiltshire erases a person's data for whatever reason it will endeavour to inform any third parties with whom AUKW has shared the data with to inform them of the erasure unless this proves impossible or involves disproportionate effort.

16.2. Data Subjects can ask, in writing, to the Chief Executive Officer, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Age UK Wiltshire) must comply with such requests within 30 days of receipt of the written request.