Data Protection and GDPR Policy

Policy Statement General Data Protection Regulations (GDPR)	The 1998 Data Protection Act brings the law into line with good practices which have been developed and promoted since the 1984 Act. At the heart of the Act is the concept of fairness – ensuring people know what is going on, using their data in predictable ways, looking after data and making sure it does not get into the wrong hands. This policy has been amended to reflect changes made by the General Data Protection Regulations (GDPR) 2018.
Responsibility Board	Implement / Review / Adhere to Policy
Chief Executive / Senior Managers	Implement / Monitor / Review / Adhere to Policy
Service Leads	Ensure staff / volunteer compliance, identify / report any breaches of policy
Staff/Volunteers	Adhere to policy / report any known breaches
Service Users	Must give permission before information can be shared/stored.
Reporting Time Limits	Immediately
Policy Approved Date	March 2018
Review Period	Annually or as a result of statutory / regulatory changes.
Next Scheduled Review	June 2020
Review Committee	Trustees / Senior Managers
Reviewed by Officer Signed, Position & Date	Wendy Botham, Head of Operations 30 July 2019
Reviewed by Board Signed, Position & Date	Nicola Sawyer, Chair 26 October 2019

Contents

1 INTRODUCTION

The 1998 Data Protection Act (DPA) brings the law into line with good practices which have been developed and promoted since the 1984 Act. At the heart of the Act is the concept of fairness - ensuring people know what is going on, using their data in predicable ways, looking after data and making sure it does not get into the wrong hands.

The changes introduced as part of the General Data Protection Regulations (GDPR), which took effect on 25th May 2018, are as follows:

- Consent is more tightly defined as: "Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her.";
- There is a change of emphasis towards an "active" agreement in relation to consent;
- GDPR strengthens the rights of data subjects, elevates the importance of openness and transparency and introduces new accountability duties; and
- The 8 DPA principles are now 6 under GDPR.

2 DEFINITION OF PERSONAL DATA

Personal data can be defined as any data relating to a living individual who can be identified from those data. This includes all data:

- Held on computer;
- Held in a relevant manual filing system;
- Intended to go into one of the above; and
- In records held by public authorities.

Definition of data subject – Anyone whose personal data is processed.

3 DATA PROTECTION PRINCIPLES

There were eight Data Protection Principles under the DPA 1998 which must be adhered to to be fully compliant with the legislation. There are now 6 under the GDPR and they require that personal data shall be:

(i) processed lawfully, fairly and in a transparent manner in relation to individuals;

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

(v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

(vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

4 FAIR PROCESSING

At least one of these must apply whenever you process personal data:

Consent - the individual has given clear consent for you to process their personal data for a specific purpose.

Contract - the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation - the processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests - the processing is necessary to protect someone's life.

Public task – the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests - the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In particular processing must be transparent and it is not permissible to deceive or mislead when obtaining the data. To satisfy the criteria for transparency there must be no surprises – the data subject must know:

- Who has the data and why the data is held;
- To whom the data may be transferred; and
- And how the data subject can exercise the right to access that information.

5 DATA SUBJECT CONSENT

(i) Before storing and/or recording personal data we must:
- give full details about what we need, why we need it, what we will use/store it for, how long we will use/store it for and who will see it;

- seek consent for each type of processing;
- keep records of how consent is given and when;
- use “opt in” rather than “opt out” – this ensures clear, active and positive consent; and
- use a script/form at first point of contact.

(ii) Consent must be freely given, specific, informed and relevant and it is valid for the duration of the active relationship. It is not permanent and can be revoked at any time which we must make all individuals aware of.

(iii) We must bear in mind the capacity of the individual to ensure the individual is giving informed consent. There are no specific guidelines but the Information Commissioner’s Office (ICO) definition of vulnerable people is, “anyone who for whatever reason may find it difficult to understand how their information is used.”

If we are unable to get informed consent for one of our service users, they don’t have a legally recognised advocate and we need to provide the service, we would need to obtain and record appropriate evidence that we are collecting and storing their data to help the individual and act in their best interests.

(iv) There are stricter conditions for sensitive data and there must be additional justification for this type of processing. We must always obtain full explicit consent.

The GDPR refers to sensitive personal data as “special categories of personal data”.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

(v) Consent does not have to be in writing but it must be explicit - we cannot rely on silence/inaction.

(vi) We must be able to demonstrate how we have obtained consent so we require an audit trail. Consent forms/scripts must be completed and recorded for all service users so that we can record how and when consent was obtained, what for and in what form.

(vii) Data protection requirements of all contracts and grant offers should be adhered to at all times. Any conflicts with the Age UK Staffordshire policy will be addressed by the Chief Executive.

(viii) Data from third parties will be managed within the requirements of this policy unless an agreed alternative process has been requested and agreed.

6 DATA SUBJECT RIGHTS

Under GDPR, you have the following rights in relation to your data:

- The right to be informed
- The right of access
- The right of inaccuracies to be corrected
- The right to have information deleted
- The right to restrict the processing of data
- The right to portability
- The right to object to inclusion of any information
- The right to regulate any automated decision making and profiling of personal data

The right to be informed
You have the right to be told how we process your data and the reasons for processing. In order to provide this information to you, we have a privacy notice.

The right of access
You have the right to access your personal information (commonly known as "data subject access request"). This enables you to receive copy of the personal information we hold about you.

If a Data Subject makes a valid Subject Access Request (SAR) the response must be issued within 30 days and we are not able to charge a fee under GDPR. A SAR is defined as: Any written request to see the information held about an individual, even if it doesn't mention the DPA.

Our procedure for dealing with SARs is documented separately in the Subject Access Request Procedure.

The right of inaccuracies to be corrected
You have the right to request any incomplete or inaccurate information we hold about you is corrected

The right to have information deleted
You have the right to have your data deleted and removed from our systems where there is no good reason for us to continuing to process it.

The right to restrict the processing of data
You have the right to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

The right to portability
You have the right to obtain the data we process about you in a machine readable format and transmit the data to a different data controller.

The right to object to the inclusion of any information
You have the right to object to the processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

If you wish to exercise any of these rights please contact the Chief Executive or Data Governance Lead.

7 MANAGING DATA PROTECTION PROCEDURES

The Chief Executive and Data Governance Lead (Head of Operations) will take overall responsibility for managing data protection. They will ensure that each line manager and service manager within the organisation is aware of their responsibilities.

The Data Governance Lead will:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; staff training and conduct internal audits; and
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

A regular audit and risk assessment of current data, and who is responsible for that data will be undertaken by the Data Governance Lead. Irrelevant or excessive data will be eliminated and a check will be made that sensitive data has been given with explicit consent.

Risk Assessments will be completed at the start of every new project/initiative to ensure that data is collected, recorded and stored compliantly.

Our Privacy Notice (Appendix 1) is held on our website, displayed in prominent places throughout our premises and it is shared with all employees, volunteers and service users.

Where there is an apparent or actual breach of Data Protection Policy this should be reported to the line manager immediately, who will inform the Chief Executive and Data Governance Lead.

When a data breach has occurred the Chief Executive will ensure any potentially affected individuals and organisations are advised of the nature and content of the breach as soon as possible and will implement all necessary actions following a thorough investigation.

A referral to the ICO will be completed within 72 hours, if appropriate. Please refer to the Breach Identification and Management Procedure for more information and guidance.

Age UK Staffordshire will ensure, as part of the induction process, that all staff, volunteers and trustees are given access to all mandatory policies and made aware of:

- What information will be kept about them, how it will be used and to whom it will be disclosed;
- How they can obtain access to such information;
- How to report concerns about data security;
- Their responsibilities for data including clients; and

- What to do in the event of a suspected data breach or failure in the workings of this policy.

All staff will be required to sign a document confirming that they have read and understood the mandatory policies.

8 SECURITY – SAFE STORAGE OF RECORDS

The organisation must take appropriate measures to guard against security breaches so we have the following in place to ensure the security of all personal data:

IT Devices

- PCs and other devices are always password protected, with regular password changes (every 90 days);
- Users lock their PC or device when they leave their desk;
- Material from computers – especially emails – are deleted at regular intervals and destruction certificates are obtained from our providers;
- Wi-Fi is password secured
- All online databases and CRM systems have secure access and different levels of permissions for different types of users.

Office

- A 'clear desk' policy is in place (please see the Clear Desk Policy for further information);
- Paper files are kept in lockable cupboards;
- All confidential paperwork which is no longer required is shredded or disposed of using a specialist company and destruction certificates obtained from our providers;
- Screens are positioned so only the user can see them, where possible. All staff are aware to be mindful of what content is displayed on their screen and who might be able to view it.
- Personal information and documents are destroyed as necessary on a regular basis in line with the Data and Records Retention Policy.

Sharing or Transferring Data

- When transferring data by post, envelopes are marked with a return address;
- Envelopes are marked ‘confidential’ and ‘for addressee only’;
- Bundles of papers are checked to ensure the right bundle is with the right covering letter;
- When sending data by email, we use an encryption service, and password protect each attachment, sending the password via a separate email.
- Personal email addresses must not be used and data in any form must not be sent to personal email addresses.

Mobile Working

- Mobile storage such as memory sticks and external hard drives are not to be used unless specifically authorised by the Chief Executive.
- Documents and data cannot be shared in any way between work and personal IT, unless specifically authorised by the Chief Executive.
- We password protect our files and folders;
- All IT hardware devices are password protected and use encryption

- There is a robust system for assigning IT devices, and ensuring they are all accounted for at reasonable intervals;
- All paper client files should be signed in and out of the office, and includes time limits for returning paperwork or electronic information to the office following client home visits (Please see our Mobile Working Policy); and
- We ensure staff members and volunteers limit what information they keep at home and it is kept secure.

Supporting Staff

- We include GDPR and IT safety in induction and mandatory training;
- We ensure all staff and volunteers know what is expected of them when handling client data;
- Our Data Governance Lead ensures that spot checks are completed at regular intervals to check data protection rules are being followed;
- Our staff know who to talk to if they identify a breach or potential breach
- Staff personnel files and records, including self-certificates for sickness absence and supervision notes are kept securely in a central location with limited and agreed access. Copies should not be kept by individuals.

9 UNAUTHORISED ACCESS AND BREACHES OF POLICY

Far more security breaches come about through inadvertent, mischievous or deliberate misuse of data by people who are entitled to have it, than by external intrusion. This means that everyone has a duty to ensure that security breaches do not occur – each line manager should ensure staff and volunteers are regularly reminded about what is meant by confidentiality and security.

Individuals who breach security may be committing a criminal offence if they "knowingly or recklessly" obtain data or allow other people access to data without authorisation. This can include gossip or such activities as conversations which allow clients details to be overheard by someone outside the organisation, or working on a train where someone else could overlook or overhear confidential information.

Any inadvertent unauthorised access or breach of this policy may lead to disciplinary action and/or prosecution and any malicious or deliberate breach will be viewed as gross misconduct.

Please read the policies and procedures previously outlined in this document for further information and guidance.

This Policy will be reviewed annually or in response to any legislative changes.

10 POLICY IMPLEMENTATION

- Staff/Volunteer/Trustee Training
- Staff/Volunteer/Trustee Induction Training
- Sharing learning from Risk Assessment Outcomes and Spot Check/Audits
- Confidentiality Audits
- Discussion in Team Meetings

- Regular email updates by GDPR Lead.

PRIVACY NOTICE

Who we are
We are Age UK Staffordshire, whose head office is at The Roller Mill, Teddesley Road, Penkridge, Staffordshire, ST19 5BD. We have offices and activities across Staffordshire, but all are part of our organisation.

What information we keep and why
We process personal data relating to clients, customers, supporters, staff, volunteers and trustees of our organisation. This is to allow us to offer services, products and help and guidance to our clients, and to be able to keep people up-to-date with our work and our plans.

We need to keep some basic information about you to be able to help you with any advice or issues you have asked us about, and to be able to offer you services or information. This will include some contact details, and a record of what you have chosen to talk to us about. This will allow us to find out the correct information, and to contact you in order to fulfil your request.

How we will contact you
If you have agreed to receive marketing and promotional information from us, we will send that out to you using the contact methods agreed with you. We will not use the information you gave us to find out more about you.

When sending information by post, we may target information or campaigns to people in specific areas of Staffordshire, based on your postcode. This is to ensure that you receive only relevant information about our work and our plans.

If you wish to change how we contact you
All our materials, whether sent out by post, email or other method, will tell you how you can stop receiving information from us.

You can stop receiving information from us at any time. To do this, you can write to us at The Roller Mill, Teddesley Road, Penkridge, Stafford, ST19 5BD, ring one of our Careline team on 01785 788 477 or email info@ageukstaffordshire.org.uk or contact us via our website at https://www.ageuk.org.uk/staffordshire/contact-us/

We aim to fulfil all requests to stop sending information within 5 working days of receiving it.

Who will see your personal data?
We will only share your information with people you have agreed to let see it. This might include people whose help we need to progress your case, such as the DWP or the local authority. We will always ask you before sharing your details. You can say no to this request.

We might want to share your details with other local groups or organisations that offer services and advice to older people in our area. This will be limited to organisations offering advice or services that you have requested that we cannot offer, or that fit directly with issues you have raised with us. Such organisations might contact you directly. We will only do this if you have agreed, and you can say no to this request.

We will never give your data away or sell it to anyone.

What data will be kept?
We are required to keep some personal data, even after we've finished dealing with your case or after you have stopped being a supporter of our work. This may include contact details, records of who we spoke to on your behalf, any correspondence, and an outline of any steps we took or advice we gave. We will keep data for a total of six years. This is to ensure that we have a record of what we did in the event of a complaint or legal claim.

At the end of six years, all non-financial data will be removed from the database and redacted so that all details of your case are removed and paper records will be securely destroyed. Organisational financial data will be securely destroyed after seven years.

We keep an overall summary of the number of people who contact us, and the types of issues people contact us about. It is not possible to identify individual cases or people from this data.

The collection of this information will benefit clients by:
- Allowing us to identify important issues that are affecting older people in our area
- Helping us to design services and projects to address need
- Focusing our campaigning and public engagement
- Ensuring we train our staff and volunteers in the areas that matter
- Tailoring our resources to the issues that matter most to our clients

How does the organisation protect data?
The organisation takes the security of your data seriously, having robust policies and controls in place. All data will be stored either on an encrypted or secure database, or paper records which are securely stored. Both paper and database information have limited access for staff. Information will not be accessed except in response to a query about our actions in the case. No decisions will be made about you based on this data and you will not suffer any detriment or harm by having it stored on our secure systems.

Seeing the information we hold about you
You can ask to see a copy of all the information we hold about you. To do this, you can write to us at The Roller Mill, Teddesley Road, Penkridge, Stafford, ST19 5BD, ring one of our Careline team on 01785 788 477 or email info@ageukstaffordshire.org.uk

If you want to complain about how we collect, store or use your data
You can contact us if you have any complaints about how we have collected, used or stored your personal data. You can write to us at The Roller Mill, Teddesley Road, Penkridge, Stafford, ST19 5BD, ring one of our Careline team on 01785 788 477, email info@ageukstaffordshire.org.uk, or contact us via our website at https://www.ageuk.org.uk/staffordshire/contact-us/

They will put you in touch with a member of the senior management team, who will oversee your complaint.