Herefordshire & Worcestershire Age UK

DATA PROTECTION & GDPR POLICY

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 – The word 'user' means anyone who uses the services of Age UK Herefordshire & Worcestershire (Age UK H&W) directly or indirectly, whether being an individual or another organisation, including Age UK H&W refers to paid staff and volunteers).

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 toindividuals;

(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 thepurposes 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 conditions must apply whenever you process personal data:

Consent - the individual has given clear consent for you to process their personal datafor 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 (notincluding 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 interestor 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 ifyou 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 (Age UK H&W) 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 validfor 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 individualis 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 beadditional justification for this type of processing. We must always obtain full explicit consent.

The GDPR refers to sensitive personal data as “special categories ofpersonal 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 recordedfor 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 Herefordshire and Worcestershire 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, an individual , a client or anyone, has the following rights in relation to their 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
An individual has the right to be told how we process their data and the reasons for processing.In order to provide this information to them, we have a privacy notice (Appendix 1).

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 a 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 itdoesn'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 aboutyou 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 continue 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 GDPR Lead.

7 MANAGING DATA PROTECTION PROCEDURES

The Chief Executive and GDPR Lead 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 GDPR Champion will:

- inform and advise the organisation and its employees about their obligationsto 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.
- be the first point of contact for supervisory authorities and for individualswhose data is processed (employees, customers etc).

A 12 monthly audit and risk assessment of current data, and who is responsible for that data will be undertaken by the GDPR Lead. Irrelevant or excessive data will be eliminated and a check will be made that sensitive data has been given with explicit consent. If more audits are needed this will be decided by the GDPR Champion and the CEO.

Risk Assessments will be completed by the Service Manager/ Project lead 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 GDPR 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 thoroughinvestigation.

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 Herefordshire & Worcestershire will ensure, as part of the induction process, that all staff, volunteers and trustees are given access to all mandatory policies and trained in Data Protection within the first week of starting and will be 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.
- What to do in the event of a suspected data breach or failure in the workingsof 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.
- Secure Wi-Fi is password protected.
- 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.
- 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.

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 Leadership Team or CEO.
- Documents and data cannot be shared in any way between work andpersonal IT, unless specifically authorised by the Chief Executive.
- We password protect our files and folders; Files and folders will be password protected.
- All IT hardware devices are password protected. There is a robust system for assigning IT devices.
- All paper client files should be signed in and out of the office and includetime limits for returning paperwork or electronic information to the office following client home visits.
- 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 GDPR Champion ensures that spot checks are completed atregular 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.

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 “knowinglyor 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.

Retention Periods

The main UK legislation regulating statutory retention periods is summarised below. If in doubt, it's a good idea to keep records for at least 6 years (5 in Scotland), to cover the time limit for bringing any civil legal action.

Client information	Document	Retention period
	Our client data, regarding sensitive and detailed information,	Data will be held for five years after completion of the final project support. Basic data is stored for life to enable us to have evidence for legacy claims.

Health and Safety	Document	Retention period
	Accident books, accident records/reports (See below for accidents involving chemicals or asbestos)	Statutory retention period 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).
	First Aid Training	Statutory retention period 6 years after employment. Statutory authority: Health and Safety (First Aid) Regulations 1981
	Fire warden training	Statutory retention period 6 years after employment. Statutory authority: Fire Precautions (Workplace) Regulations 1997.
	Health and Safety representatives and employees' training	Statutory retention period 5 years after employment. Statutory authority: Health and Safety (Consultation with Employees) Regulations 1996; Health and Safety Information for Employees Regulations 1989.

Finance	Document	Statutory Retention
	Income tax and NI returns	Statutory retention period income tax records and correspondence with HMRC Not less than 3 years after the end of the financial year to which they relate. Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).
	Accounting records	Statutory retention period 3 years for private companies, 6 years for public limited companies. Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.
	Payroll wage/salary records (also overtime, bonuses, expenses)	Statutory retention period 6 years from the end of the tax year to which they relate. Statutory authority: Taxes Management Act 1970.

Human resources	Document	Retention period
	Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence (also shared parental, paternity and adoption pay records)	Statutory retention period 3 years after the end of the tax year in which the maternity period ends. Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended, Maternity & Parental Leave Regulations 1999.

	Subject access request	Statutory retention period 1 year following completion of the request. statutory authority: Data Protection Act 2018.
	Whistleblowing documents	Statutory retention period 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately. Statutory authority: Public Interest disclosure Act 1998 and recommended IAPP practice
	Working time records including overtime, annual holiday, jury service, time off for dependents, etc	Statutory retention period 2 years from date on which they were made.
	Flexible Working requests	Recommended retention period: 18 months following any appeal. This is because a further request cannot be made for 12 months following a request plus allowing for a 6 month tribunal limitation period on top.
	Parental leave	Recommended retention period: 18 years from the birth of the child.
	Personnel files and training records (including formal disciplinary records and working time records)	Recommended retention period: 6 years after employment ceases but note that it may be unreasonable to refer to expired warnings after two years have elapsed
	Recruitment application forms and interview notes (for unsuccessful candidates)	Recommended retention period: 6 months to a year. Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job

		applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicant's documents will be transferred to the personnel file in any event.
	Redundancy details, calculations of payments, refunds, notification to the Secretary of State.	Recommended retention period: 6 years from the date of redundancy.
	References	Recommended retention period: At least one year after the reference is given to meet the limitation period for defamation claims.
	Right to work in the UK checks	Recommended retention period: Home Office recommended practice is 2 years after employment ends.
	Senior executives' records (that is, those on a senior management team or their equivalents)	Recommended retention period: Some records may be needed permanently for historical purposes. Retain personal records, performance appraisals, employment contracts etc for 6 years after the employee has left to reflect the main limitation period.
	Statutory Sick Pay records, calculations, certificates, self-certificates, occupational health reports	Recommended retention period: 6 years after the employment ceases.
	Termination of employment, for example early retirement, severance or death in service	Recommended retention period: At least 6 years although the ICO's retention schedule suggests until employee reaches age 100
	Terms and conditions including	6 years after employment

	offers, written particulars, and variations	ceases or the terms are superseded.

Appendix 1

PRIVACY NOTICE- General

Who we are

We are Age UK Herefordshire &d Worcestershire, whose head office is at Malvern Gate, Bromwich Road, Worcester. We have offices and activities across Herefordshire and Worcestershire, 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 Herefordshire or Worcestershire, 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 youcan stop receiving information from us.

You can stop receiving information from us at any time. To do this, you can write to us at Malvern Gate, Bromwich Road, Worcester, WR2 4BN. ring a member of our Referral Hub on 0800 008 6077 or email or contact us via our website at Age UK Herefordshire & Worcestershire | Contact us.

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

Who will see your personal data?

We will only share your information with people you have agreed to see it. This might include people whose help we need to progress your case, such as the Department of Work and Pensions 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. . We willonly do this if you have agreed, and you can say no to this request. However, such organisations might contact you directly

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.

Q-Is the above para consistent with the first row in the 'retention period 'table below?

We keep an overall summary of the number of people who contact us, and the types of issues people contact us about. We will only identify people if required in a legacy claim. 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

Q-Any legal or charity laws that demand that we keep some types of data?

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 andyou 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 Malvern Gate, Bromwich Road, Worcester, WR2 4BN ring a member of the Referral Hub on 0800 008 6077 or email Referralhub@ageukhw.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, Malvern Gate, Bromwich Road, Worcester, WR2 4BN ring a member of the Referral Hub on 0800 008 6077 or email Referralhub@ageukhw.org.uk,
The referral hub will put you in touch with a member of the senior management team, who willoversee your complaint.

Appendix 2:

Privacy Notice – Job Applicants / Employees and Volunteers

At Age UK H&W ("the Charity"), we are committed to protecting and respecting your privacy. As part of any recruitment process, The Charity collects and processes personal data relating to job applicants. The Charity is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information do we collect?

The Charity collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number.
- details of your qualifications, skills, experience and employment history.
- information about your current level of remuneration, including benefit entitlements.
- whether or not you have a disability for which the Charity needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

The Charity may collect this information in a variety of ways. For example, data might be contained in application forms, CVs, or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

We may also collect personal data about you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

For what purpose will your data be used?

The personal data you provide in your application and as part of the recruitment process will only be held and processed to facilitate the selection process and in connection with any subsequent employment.

Your personal data may be used to assess your application for employment with the Charity in order to verify your information, to conduct reference checks, to communicate with you and to inform you of further career opportunities. In some cases, we need to process data to ensure that we are complying with its legal obligations. For example, it is mandatory to check a successful applicant's eligibility to work in the UK before employment starts.

The Charity may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics.

We may also collect information about whether applicants are disabled in order to make reasonable adjustments for candidates who have a disability.

In the event of your application resulting in an offer of employment and your acceptance of a position with the Charity, the data collected will become part of your employment record and will be used for employment purposes.

Who has access to data?

Only selected employees of the Charity - such as senior management team members, potential future line managers or HR and Payroll staff - have access to your personal data.

We will not share your data with third parties unless your application for employment is successful and we make you an offer of employment.

We ~~will~~ may share your data with former employers to obtain references for you

How does The Charity protect data?

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused, or disclosed, and is not accessed except by our employees in the proper performance of their duties.

For how long does The Charity keep data?

Your personal data shall not be kept for longer than is necessary for the recruitment process. Therefore, unsuccessful application data will be deleted six months after the completion of the hiring process.

In addition to using your data for the position for which you have applied, the Charity may wish to retain and use your application data to consider you for other future employment opportunities for which you may be suited. We will ask for your consent before we keep your data for this purpose and you are free to withdraw your consent at any time.

Your Rights

You may exercise the following rights in relation to your candidate data:

- access and obtain a copy of your data on request.
- require the Charity to change incorrect or incomplete data.
- require the Charity to delete or stop processing your data, for example, where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where The Charity is relying on it's legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact hr@ageukhw.org.uk.

If you believe that the Charity has not complied with your data protection rights, you can complain to us or the Information Commissioner, using any of the contact methods below:

Age UK H&W:
Telephone: 0800 008 6077 **Email:** Aweaver@ageukhw.org.uk

Information Commissioner:
Telephone: 0303 123 11113 **Website:** https://ico.org.uk/make-a-co

Appendix 3

Privacy Notice
Clients- Privacy Notice.

Who are we?
Age UK Herefordshire & Worcestershire (Age UK H&W) is a trading name of Age Concern Herefordshire & Worcestershire, a registered charity (number 1080545) and company limited by guarantee, registered in England and Wales (Number 3942023). The Registered Office is Age UK H&W, Malvern Gate, Bromwich Road, Worcester. WR2 4BN.

This privacy notice applies to Age UK H&W and other associated companies where applicable.

When individuals provide their data to Age UK H&W, we act as a Data Controller, regarding the storage and processing of any information provided to us as an organisation.

Data we may process
The data we process will depend on the services you require. It will generally include personal data such as name, date of birth and contact details, and in some cases sensitive data such as medical details when necessary.

What does Age UK H&W do with the information?
Age UK H&W is committed to the secure storage and processing of your personal and sensitive data as required under the Data Protection Act 2018 and General Data Protection Regulation (GDPR). The information you pass to Age UK H&W will be used to provide services which are appropriate to your needs and then stored securely. When you are no longer a client or a specific service has finished your data will be securely destroyed. Your data will not be passed to any third parties without your consent and Age UK H&W will never sell your data. It may sometimes be necessary to pass your details to other suitable Age UK H&W services where you have given consent. A detailed Privacy Statement is available on request to help you clarify the way we will use your information.

Our client data, regarding sensitive and detailed information, will be held for five years after completion of the final project support. Basic data is stored for life to enable us to have evidence for legacy claims.

If you have given consent for us to keep in touch with you, the data you have provided may be used to keep you updated with news from Age UK H&W, our services and charitable activities.

You may unsubscribe or change how we communicate with you at any time. Please email our office at qualityassurance@ageukhw.org.uk, or call us on 01905 740950, if you wish to make any changes.

Procedures for Maintaining Your Rights
Age UK H&W have procedures in place to ensure all the rights that individuals have regarding use and storage of your data are covered. This includes your right to access the

data Age UK H&W hold about you. Data is available as a hard copy or electronically in an easy to read format, with an emphasis on confidentiality. You have the right to request amendments of the data held about you if the information is incorrect or incomplete.

If you are currently receiving information from Age UK H&W and no longer wish to do so, please contact our office; details are below. You also have the right to request your data is deleted.

If you require further information on how your data is used and stored, please refer to our Privacy Policy and Privacy Statement at www.ageukhw.org.uk

Complaints
If you believe your data is being dealt with incorrectly or inappropriately you have the right to complain to Age UK H&W or the Information Commissioner's Office (ICO). Please contact our office for further information.

Contact details
Age UK Herefordshire & Worcestershire
Malvern Gate
Bromwich Road
Worcester
WR2 4BN
01905 740950
Email: qualityassurance@ageukhw.org.uk
www.ageukhw.org.uk