AGE UK EXETER

Controlled Document
Document Name: Data Protection Policy

Document Version Number: 16

Agreed by Risk and Quality Committee: 30.07.24

Approved by Board of Trustees on: 20.08.24

Review Schedule: Every three years

Next review due: July 2027

Owner (Responsibility) CEO

Amendments to: Governance Lead

Revision History: See end of document

Document location: www.ageuk.org.uk/exeter/about-us/policiesandguidelines

Document Description
This document outlines our legal requirements under the UK General Data Protection Regulations and the processes by which Age UK Exeter (AUKE) meets them.

Implementation and Quality Assurance
Implementation is immediate and this policy shall stay in force until any alterations are formally agreed.

The policy will be reviewed every three years by the Board of Trustees, 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. If you have any comments or suggestions on the content of this policy, please contact the CEO on info@ageukexeter.org.uk or at Age UK Exeter, The Sycamores, Mount Pleasant Road, Exeter, EX4 7AE, 01392 202092.

Data Protection Policy

1. Introduction

Data protection is about ensuring people can trust organisations to use their data fairly, responsibly, and transparently. The UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018, applies to processing carried out by organisations operating within the UK. The Information Commissioners Office (ICO) regulates data protection in the UK.

The following is not a definitive statement on the Act but seeks to interpret relevant points where they affect AUKE.

The Act covers both written and computerised information and the individual's right to see such records.

It is important to note that the Act covers all records relating to clients, staff, and volunteers.

All AUKE staff and volunteers are required to follow this Data Protection Policy and Procedures. Failure to do so may lead to disciplinary action.

The Chief Executive has overall responsibility for data protection within AUKE, 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

Processing of information – how information is held and managed.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. AUKE is the data controller for the purposes of the Act.
Data Processor – an individual handling or processing data.
Personal data – any information about a particular living individual which can identify who they are. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official, or member of the public.
Special categories of personal data – Some of the personal data processed can be more sensitive in nature and therefore requires a higher level of protection. The GDPR refers to the processing of these data as 'special categories of personal data'. This means personal data about an individual's:

- race
- ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership

- genetic data
- biometric data
- health data
- sex life or sexual orientation.

3. Data Protection Principles

The UK GDPR sets out seven key principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of our approach to processing personal data.

Article 5(1) requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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.
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date or erased or rectified without delay.
- 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.
- 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.

Article 5(2) adds that:

- The controller shall be responsible for and be able to demonstrate compliance with the GDPR.

These principles lie at the heart of UK GDPR. They don't give exact rules or numerical guidelines but rather embody the spirit of the general data protection regime and it is up to individual organisations to interpret them for practice and define their lawful basis for processing.

4. Individual's Rights

The UK GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

5. Procedures

Lawful Basis

At AUKE, our lawful basis for processing information is:

- Legitimate Interests
- Consent
- Public Task in terms of Information and Advice form filling.

Consent

Consent means giving individuals real choice and control. It must be explicit, specific and requires a positive opt-in. An organisation must keep their consent requests separate from other things and keep an evidence trail of decisions. It must be easy to withdraw consent if an individual wants to.

Obtaining Consent

Consent can be obtained in several ways depending on the nature of the interaction. Best practice is to obtain consent at the beginning of an exchange, but if this is not viable, it can be obtained at the next appropriate meeting, if a decision is not vital and can be postponed. Though written consent is the optimum, verbal consent can be taken if the situation means it is the only viable option and if an accurate, dated evidence trail is kept. Consent obtained for one purpose cannot automatically be applied to all uses.

At AUKE we have a General Data Information and Consent Form that covers, legitimate interests to store, consent to share, consent to contact next of kin in an emergency, and consent for mailings. We also have a Photography Consent Form that covers photography, videography, and case studies. Such media could be used for, but is not limited to, publicity

material, press releases, social media, and our website and on the website of our partner organisations if appropriate. If the subject is less than 18 years of age, then parental/guardian consent should be sought. Photography consent is deemed valid from when it is given to when consent is withdrawn if applicable. Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by AUKE, then the Service Lead should discuss this with the CEO at the earliest opportunity.

Consent and mental capacity

In most circumstances, AUKE's General Data Information and Consent Form will be used to obtain consent. A relative, carer, trusted individual or AUKE member of staff can assist with this if they are comfortable the client has capacity. The form can be marked as a signature in any way that authorises consent and denotes understanding. In compliance with the Mental Capacity Act (MCA), AUKE understands that capacity is time and decision specific and therefore if a decision is not urgent, it may be that the person will have capacity to make the decision at another point in time. AUKE will always seek to empower and listen to the individual and allow them to give consent if possible. Verbal consent can also be recorded if the only viable option.

For our Information and Advice Service, Lasting Power of Attorney's will need to be seen if a request is made to process an individual's personal information on their behalf.

To deliver a service, in line with the MCA, if consent cannot be sought and a decision is vital, the family, carers or trusted individuals will be consulted, and a decision made whether to offer the least restrictive option in the person's best interests. Good documentation of all decisions of this kind must be kept. Please see our Mental Capacity Act Policy for further information.

Data Security and Data Sharing

It is an offence to disclose personal information 'knowingly and recklessly' to third parties. Every care is taken within the organisation to ensure data security as detailed in the sections below. All personal data is treated as confidential and only shared with outside agencies if express consent has been given to do so. Special categories data is treated with the utmost care and only stored on our main secure database (Charitylog) or securely on a home support workers work mobile phone (client information sheets), password protected. Personal information would only be shared without consent if it related to criminal proceedings or a safeguarding issue and then only on the express permission of the Chief Executive Officer and Service Manager. Personal information should only be communicated within AUKE's staff and volunteer team on a strict need to know basis. Care should be taken with those conversations containing personal or special categories of personal information that they are not overheard by people who should not have access to that information. Please see our Confidentiality Policy for more information.

For our 'Hospital to Home' project, commissioned by the NHS, we have a Data Protection Impact Assessment (DPIA) in place which describes all parts of data exchange within the project.

We are also making a move in the organisation to completing data impact assessments on inception of a new project/programme of work. These will describe data flow, risk mitigation and any issues or concerns. Please see a copy of the template in the appendix.

6. Equality, Diversity, and Inclusion

AUKE does not routinely monitor equality, diversity and inclusion statistics at present. The organisation ensures that staff are trained in diversity and inclusion every two years and that clients can access our services whatever their circumstances. AUKE also invests in a Satisfaction and Wellbeing survey annually to better understand the needs and experiences of its service users.

Use of Files, Books and Paper Records

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 should be kept in locked cabinets/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. If work involves a staff member having personal/and/or special categories of personal data at home or in their car, the same care needs to be taken. Any breaches must be reported to the Governance Lead as detailed below.

7. Disposal of Scrap Paper, Printing or Photocopying Overruns

Care must be taken that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Staff must not keep or use any scrap paper that contains personal information but ensure that it is confidentially shredded.

AUKE has a contract with Paperchain, an organisation that supplies confidential waste services to destroy confidential waste. Certificates of Destruction are issued after every collection and can be viewed in the Data Protection file in the Admin Office.

If staff are transferring papers from home, or from a client's home to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents, they should be carried out of sight and treated as confidential material.

8. Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Firewalls and virus protection is installed to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Confidential documents should only be stored in Teams or on cloud-based systems and not on individual computers. Download folders and emails have automatic deletion in place to

aid data security and cleansing. Data is also segmented across the organisation to aid data security and safeguard against breaches and hacks. See our Systems below. The Operations Manager also has remote access which improves the security of our systems and allows laptops to be wiped remotely if necessary.

Where computers or other mobile devices are taken for use off the premises the device must be password protected. Care should be taken when staff work from home, that they protect confidential information and documents.

Our computer systems are insured under our Computer/Engineering Policy with cover for computer virus, hacking and denial of service attacks up to the value of £100,000.

We also have a stand-alone Cyber Security insurance policy that gives us access to 24-hour support in the event of a cyber-attack and assists us with risk mitigations.

9. Systems

When commissioning new systems, AUKE will satisfy themselves as to the compliance with data protection principles and robustness of the providers. A data impact assessment will be carried out where appropriate.

Charitylog

Charitylog, hosted by Dizions Ltd, holds data about our clients, volunteers, and staff. Access is password protected and restricted to named users, with levels of access for each user set to a 'need to know' basis appropriate to their job.
Charitylog has regular penetration tests to ensure nothing has become out of date and they use reputable and secure data centres in the UK (Rackspace and AWS). The data is all processed in the UK. They have ISO27001 data security accreditation and Cyber Essentials Plus.

Charitylog provide a separate database for staff training purposes. This gives the opportunity to look at things or train people without the risk of inputting incorrect or made-up data into the live database. Charitylog has also allowed us to shape our own consent settings and easily allows the charity to fulfil subject access requests and 'forget me' requests. The Operations manager backs up our main files on Charitylog weekly.

Microsoft Teams/Microsoft 365

Microsoft Teams as part of Microsoft 365 and Office 365 services follows robust security practices, such as:

- Trustworthy by design
- Encryption
- Common Threat Mitigation
- Compliance.

AUKE also utilises Outlook as part of Microsoft Office suite of applications.

It is noted that Microsoft has monopoly of the market so a cyber-attack on its systems would be huge and beyond the boundaries of just AUKE.

Xero

Xero is utilised by the finance team for financial management and accounting purposes. Xero encrypts business information and replicates it in several locations online. This means that it is safe and secure. Multi-factor authentication (MFA) adds an additional layer of security. No one has access to the charity's data unless they are invited into the account. The finance manager has control over what users can see and do in Xero. Xero is backed up and protected online in the cloud and can be accessed from any location with an internet connection. All data centres have robust physical security controls as well as 24/7 monitoring and surveillance.

People HR

AUKE also utilises People HR for holiday requests. People HR is hosted in the cloud meaning it is available anywhere there is a browser and internet connection. People HR is owned by Access UK Ltd and is registered with the Information Commissioner's Office. Data is stored in Telehouse N2 (London). All data centres only provide 'co-location' services because the Cloud Hosting Services team manage the environment. It is protected using multiple layers of technology which is monitored 24/7. Physical controls include biometric access controls, man trap access, admission by appointment, 24/7 security staff and surveillance. Back-ups are run daily and stored in encrypted format. They are stored for 90 days. People HR is also ISO 27001 accredited.

The Box

AUKE uses Box to collate and manage Board materials, finance documents, finance committee papers and other confidential materials. Box adheres to high industry standards for security with secure data centres, daily back up, and encryption. Box is also SAS70 Type 2, and Safe Harbour certified.

Payment Sense

AUKE uses payment sense to manage digital payments. The charity has three ipads specifically used for this purpose. These are centrally managed within the finance team and password protected.

Payment sense uses a virtual terminal to process electronic payments over the phone securely. The payment gateway lets the charity take payments online or over the phone. When clients are ready to pay, it sends their card details to payment sense via an encrypted connection, and payment sense sends them onto the client's bank to confirm there are enough funds. This all happens within seconds and the charity can approve payment. It uses the latest security software and fraud protection and has 24/7 support available should the charity need it.

Mobile devices

AUKE's mobile phone network is managed by Radius. Capable devices are managed by AUKE using encryption, location, and tracking capabilities. These devices are equipped with remote remedial actions such as remote tracking and wiping to ensure data security.

Competitive Solutions
Competitive Solutions are an out-sourced company that AUKE uses for fundraising and bid writing. AUKE has satisfied itself with the consultancy agreement, particularly in terms of data protection.

Printer
The main printer at Sycamores is on five-year lease. Staff are encouraged to collect printed documents immediately and confidentially shred any misprints. The CEO, SMT and Governance Lead have password protection to ensure the confidentiality of potentially sensitive documents.

10. Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc). The communication may be in any of a variety of formats including mail, telemarketing, and email. The responses will be recorded to inform the next communication. AUKE will not share or sell its database(s) with outside organisations.

AUKE holds information about clients, volunteers and supporters on its main database, Charitylog. At any point in time, a consent report can be generated which will give up-to-date contacts who have given their consent to receive newsletters or information about upcoming events or fundraising requests. Individuals' communication preferences and accessible information requirements can also be viewed on Charitylog under their general details.

We recognise that clients, staff, volunteers, and supporters for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their personnel record, and they will be excluded from future contacts.

11. Privacy Statements

An Organisational Privacy Statement will be published on our website. Please see copy in Appendix 1. All clients will receive a summary privacy notice when they sign up for service. This notice will explain what information we hold and why. Staff and volunteers will receive a detailed privacy notice upon appointment explaining the various pieces of information held and why.

12. Disclosure and Barring Service

All AUKE staff and volunteers (who are regularly involved with vulnerable adults) will need a Disclosure & Barring Service (DBS) check on appointment. AUKE trustees will also be

subject to DBS checks. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the CEO and Service Manager. If there is a positive disclosure the Chief Executive will discuss this, anonymously, with the Chair of the Risk and Quality Committee, Service Manager, and our insurers to assess the risk of appointment. Trustees and insurers should not see the report itself. Please refer to our DBS Policy for more information. Staff and volunteers who are subject to DBS checks, must disclose any convictions, cautions, reprimands, and final warnings which are issued to them after the DBS check has taken place. DBS checks will be refreshed every three years.

13. Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy. When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All electronic data, e.g., documents and programmes related to work for AUKE should not be stored on any external hard disk or on a personal computer. All staff have access to Microsoft Teams and should be able to work safely and securely from home if necessary.

When using text messages to communicate with staff it is important to consider the possibility that someone else may read a text message that is sent regarding a client (e.g. a family member, the phone may be passed on, sold, or stolen and end up in the possession of someone else). Staff should consider what information it is appropriate to include, only the minimum amount of personal data for the purpose should be communicated via text. Best practice would be to use Charitylog number, but if not possible, first name and initial of surname should be used rather than using client's full name. Texts should be regularly deleted from a device, and mobile phones should be password protected.

When sending emails or other electronic communications to outside organisations, e.g., social worker or hospital staff, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number, such as social services number) are used where possible. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork concerning clients or confidential details should always be treated as confidential. Brown envelopes are in use in the office and papers should be treated as private and confidential when at home, in a client's home or in transit. The organisation also advocates a 'clear desk policy' at the end of the day and when away from one's desk.

Home support workers will only receive client information in password protected emails/files and these should be deleted as soon as advised to do so.

14. Retention of Records

We have a detailed AUKE Data Retention Schedule (please see separate document). All data will be cleansed after the appropriate timescale.

15. What to Do If There Is a Breach

If a staff member or volunteer discovers, or suspects, a data protection breach they should inform their line manager and the Governance Lead immediately. A member of the SMT or Governance Lead will then complete a risk assessment and aim to contain the breach. From this, they will consider whether the breach needs to be reported to the Information Commissioner's Office (ICO). If deemed necessary, serious breaches must be reported to the ICO within 72 hours. The ICO can also give advice via their helpline. The Governance Lead will record details of the breach and a meeting will take place to inform future mitigation. It may also be necessary to consider whether our insurers need to be informed.

In the event that the breach involves clients receiving a service commissioned by Devon County Council or the NHS, the commissioning authority should be informed by the Chief Executive or Services Manager by emailing keepdevonsdatasafe@devon.gov.uk or by phoning the commissioner's Information Governance Team.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

16. Subject Access Requests (SARs)

Data subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (AUKE) must comply with such requests within 30 days of receipt of the written request and keep adequate records of all proceedings.

17. Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence.

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further information is available at www.ico.org.uk

Details of the Information Commissioner

The Information Commissioner's office is at:
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Data Protection Help Line: 0303 123 1113

Or use their live chat service at www.ico.org.uk

Revision History

Revision date	Summary of Changes	Other Comments
14 May 2019	Approved by Board of Trustees	
May 2021	Internal review	
November 2022	Update with attention to ICO, including Legitimate Interests Assessments, Privacy Statement, and separate creation of Data Retention Schedule	
June 2024	Update to detail new systems in place, current best practice, and new templates and structures to outline where data resides in the organisation and how we mitigate against risks.	

Appendix One

Age UK Exeter Organisational Privacy Notice

Age UK Exeter is a local charity that has worked across Exeter for over 30 years. Our mission is to enable older people to make the most of life, whatever their circumstances.

Our contact details:

Sycamores, Mount Pleasant Road, Exeter, EX4 7AE.

Telephone: 01392 202092

Email: info@ageukexeter.org.uk

What type of information we have:

We collect and process personal information relating to clients, supporters, staff, volunteers, and trustees of our organisation. This may include personal identifiers, contacts and characteristics and include service history and/or services accessed and medical information if appropriate. This is to allow us to offer services, products, help and guidance to our clients and to be able to keep people up to date with our work and plans.

How we get the information and why do we have it:

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- You give us your information so that we can provide a service to you.
- You give it so we can fulfil a request.
- So that you can support us.
- Because you would like to receive communications from us.
- You would like to become a staff member, volunteer, supporter, or trustee.

We may also receive information indirectly, for example, if you are referred to one of our services or use the national volunteering hub.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

- Legitimate Interests
- Consent

Please note, you can withdraw your consent at any time by contacting info@ageukexeter.org.uk or telephoning 01392 202092.

What we do with the information we have:

We use the information that you have given us in order to deliver services to you, fulfil your request to us, provide you with information or advice or to keep you up to date with the charity, fundraising and our plans and developments.

If you have used our services, we may on occasion share basic demographic and service information with Age UK the national charity so they can help us monitor and ultimately improve the services we provide. The information we share will not include your name or

contact details, unless you give us your consent to do so for a specific purpose, such as sharing your story. When we do share this information, we do so under the lawful basis of legitimate interest.

In other circumstances, we will only share your details with other agencies if express consent has been given or if there is a safeguarding concern or an offence has been committed. Then and only then, we would have to share information with the advice and authorisation of our Chief Executive Officer.

How we store your information:

Your information is stored securely by us on CharityLog, our online database hosted by Dizions Ltd.

If you are in receipt of one or more of our services, have worked or volunteered for us, we will hold your data for ten years after you cease to receive a service or work for us.

If you are a supporter of Age UK Exeter, we will hold information about your donations for six years after you stop supporting us or as soon as you withdraw consent or ask to be forgotten, we will anonymise your data.

You can see full information about our data retention in our Data Protection Policy available at www.ageuk.org.uk/exeter/about-us/policiesandguidelines or by requesting a copy of our Data Retention schedule.

Your data protection rights:

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal data in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

If you make a subject access request, we have one month to respond to you.

Please contact us at info@ageukexeter.org.uk or on 01392 202092 if you wish to make a request or ask to be put through to the Governance Lead.

How to complain

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113

Appendix Two

AUKE Data Impact Assessment

Aim and outline of project/piece of work	
Data flow/processing (describe what data will be used in the project, what will this involve, consider any special category data)	
Basis for processing?	
Does the processing achieve the purpose? How will we ensure data quality and minimisation?	
Data sharing (describe data to be shared, how and when)	
Client information (how are clients kept informed? Is the service/project covered by a privacy notice?)	
Risk mitigation/current controls	
Data retention	

Challenges/risks/further considerations	
Does this project require further expertise to manage the data effectively?	
Who to contact in case of breach	
Date incepted	
Date for review	