Data Protection and Information Governance Policy

Introduction

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

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect Age UK Gloucestershire (AUKG).

The Regulations cover both written and computerised information and the individual's right to see such records. It is important to note that the Regulations also cover records relating to staff and volunteers.

All Age UK Gloucestershire colleagues and volunteers are required to follow this Data Protection Policy at all times.

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

Relevant Definitions

- Processing of information – how information is held and managed.
- Information Commissioner – formerly known as the Data Protection Commissioner.
- Notification – formerly known as Registration.
- 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. Age UK Gloucestershire is the Data Controller for the purposes of the Act.
- Data Processor – an individual handling or processing data.
- Personal data – any information which enables a person to be identified.
- Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Charity.
- Artificial intelligence – Broad term for technology that allows computers to do tasks which usually need human thinking. Like learning, solving problems or making decisions. These fall into six general categories:
    - Automation AI – automate repetitive or routine tasks – such as Microsoft Power Automate or Zapier
    - Generative AI (Gen AI) – to create new content – such as ChatGPT or Copilot
    - Predictive AI – for forecasting outcomes – such as SAS Advanced Analytics
    - Data analysis AI – examine large sets of data – such as PowerBI
    - Conversational AI – chatbots and virtual assistants – such as AccessAva
    - Computer Vision AI – interpreting visual data – such as OpenCV

Data Protection Principles

As data controller, AUKG is required to comply with the principles of good information handling. These principles require the Data Controller to:

1. Process personal data fairly, lawfully and in a transparent manner.

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

Consent

AUKG must record an individual's consent to storing certain information (known as 'personal data' or 'special categories of personal data') on the individuals file. For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

1. The racial or ethnic origin of the Data Subject.
2. His/her political opinions.
3. His/her religious beliefs or other beliefs of a similar nature.
4. Whether he/she is a member of a trade union.
5. His/her physical or mental health or condition.
6. His/her sexual life.
7. The commission or alleged commission by them of any offence.
8. Online identifiers such as an IP address.
9. Name and contact details.
10. Genetic and/or biometric data which can be used to identify an individual.

Special categories of personal information collected by AUKG will, in the main, relate to physical and mental health. Data is also collected on ethnicity and held confidentially for statistical purposes.

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

AUKG will always seek consent where personal or special categories of personal information is to be held. It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity. If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the relevant Manager or Chief Executive for advice.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the contact and consent must be recorded on or maintained with the electronic case records:

- face-to-face
- written
- telephone
- email

Face-to-face/written – A pro-forma should be used.
Telephone – Verbal consent should be sought and noted on the case record.

E-mail – The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained in relation to information needed for the provision of that service, separate consent would be required if, for example, sending out communications or updates or our wider services and fundraising.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded in an electronic record (e.g. Charitylog). The verbal consent is to be recorded in the appropriate fields on the electronic record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by AUKG then this should be discussed with the relevant manager at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information:

1. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.
2. It is a condition of receiving a service that requires us to hold personal details that consent must be gained in order to allowing us to hold such information.
3. Individuals may also consent for us to share personal or special categories of personal information with other supporting agencies (e.g. Adult Social Care, DWP, other charities) on a need to know basis.
4. An individual's consent to share information should always be checked before disclosing personal information to another agency.
5. Where such consent does not exist, information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk of harm to the individual or others. In either case permission of the Chief Executive or relevant Manager should first be sought.
6. Personal information should only be communicated within AUKGs colleague and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Diversity Monitoring

In order for Age UK Gloucestershire to monitor how well our colleagues, volunteers and beneficiaries reflect the diversity of the local community we may request that they complete an Equality and Diversity Monitoring form or provide data pertaining to the same. The completion of the form or provision of this data is voluntary, although strongly encouraged. Responses are securely stored and held for statistical purposes.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept to a minimum and in locked cabinets/drawers overnight and care should be taken that personal and special

categories of personal information are not left unattended or in clear view during the working the day. If your work involves you having personal, and/or special categories of personal data in hard copy outside of the office location, the same care needs to be taken.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be sensitive. Any scrap paper that contains personal information is to be shredded or disposed of as confidential.

If you are transferring papers from your home, or a client's home, to the office for shredding or confidential disposal this should be done as soon as possible. When transporting documents they should be carried out of sight and as securely as possible.

IT Systems

Access to AUKG IT systems and hardware is password protected. Further databases, systems and sources of personal and special categories of data are restricted by password protected application access to authorised individuals only.

Computer monitors, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. Computers should be locked at all times when unattended.

Firewalls and virus protection are employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records. All documents should only be stored on the AUKG server or commissioned cloud-based systems and not on individual computers.

Cloud Services

When commissioning cloud based systems, AUKG will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers in line with our own obligations and those of the contracts/commissioners with which we engage.

AUKG currently uses the following cloud based data management system to hold and manage information about its colleagues, beneficiaries and supporters. These are approved and AUKG is satisfied with the security levels in place to protect its data.

1. Charitylog

Charitylog, hosted by Dizions Ltd, holds data about our beneficiaries and volunteers. Access is password protected and restricted to named users, with level of access to each user on a 'need to know' basis to be able to carry out their job. Charitylog is accredited to ISO 27001 Information Security Standard. They are also accredited to the International Quality Management Standard ISO 9001 and are registered with the Information Commissioners Office. Charitylog is also signed up to Cyber Plus Essentials.

2. Breathe HR

Breathe, hosted by Centurion Software Ltd, holds colleague personnel data relating to personal information, work related information such as one to ones/objectives, holiday booking, DBS and sickness absence information. Access is password protected and limited so that only those who are entitled to access information can see it and employees can manage their own data. Breathe HR is managed by HR Solutions.

3. iHasco

iHasco, hosted by iHasco Ltd, is a staff training system, which provides online interactive health and safety training, as well as a Learner Management System to log colleague training completed. Access is restricted to the Leadership and Management Team only for the Learner Management system, and the information is only used to record mandatory training. iHasco only hold colleague names and email addresses, no other personal data is held by them.

4. Blackbaud eTapestry CRM

eTapestry, hosted by Blackbaud is used as the fundraising CRM for communication, relationship and cultivation purposes. It is used to store supporter data (including employee and volunteers) personal details, funder organisational details, pledges, giving history, communications (mass and individual such as offer letters, impact reports), communication preferences (consent) and Gift Aid Declarations.

5. Xero

Xero is a cloud based finance software It is used to store financial transactions, supplier and staff banking details and budgeting information. This is managed and supported by PEM.

6. Dext

Dext is a cloud based financial processing system linked to Xero to process invoices and expenses. It stores financial data and is managed and supported by PEM

7. Microsoft 365 Copilot

Commented [BL1]: It's now called Copilot 365

Microsoft Office is our core system which is a mix of application and cloud based. Where possible data and activity should be kept within the Microsoft environment to ensure a greater level of security. Access is managed by CSG IT.

8. Smartsheet

Smartsheet is a speadsheet based cloud system which we hold business plan, policies and objectives in a central location. Access is limited to Leadership Team, with open reports produced for Board members.

9. Canva

Canva is a cloud based system for designing documents. AUKG have a charity licence and can provide access to this to support design work as appropriate. AUKG work developed outside of the AUKG licence must not be carried out.

10. **Exclaimer Signature Update Agent**

Exclaimer is an online agent allowing us to synchronise email signatures centrally. Managed by CSG and Comms team

As the organisation progresses its use of Cloud Based Systems the same level of due diligence will apply to their selection, commissioning and implementation.

Wider Communications (incl. Fundraising Correspondence, Campaigns and Appeals)

Fundraising Correspondence is 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 letter or email.
The response received (if any) will be recorded to inform the next communication. AUKG will not share or sell its database(s) with any third party.

AUKG holds information on our colleagues, volunteers, clients and other supporters, to whom we will from time to time send copies of newsletters and details of other activities that may be of interest to them. Specific consent to contact will be sought from our colleagues, clients and other

supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications or where a 'legitimate' interest assessment is not considered appropriate.

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

The following statement is to be included on any forms used to obtain personal data:

We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 01452 422660, writing to Age UK Gloucestershire, Henley House, Barnett Way, Gloucester, GL4 4RT or by sending an email to enquiries@ageukgloucestershire.org.uk

Privacy Statements

Whenever we are gathering personal and/or special categories of personal data we will provide a Privacy Statement including the following information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for direct correspondence notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

Our Privacy Statement is available on request and is also published on our website.

Personnel Records

The Regulations apply equally to volunteer and colleague records. AUKG may at times record special categories of personal data with the volunteer's consent or as part of a colleague's contract of employment.

For colleagues and volunteers who are regularly involved with vulnerable adults, it will be necessary for AUKG to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer database or elsewhere. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Management Team and HR. If there is a positive disclosure the Chief Executive will discuss this, anonymously, with the Chair of Trustees and our insurers to assess the risk of appointment. Trustees and insurers should not see the report itself.

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 AUKG should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer they should be saved onto a USB drive issued by AUKG which is encrypted and password protected.

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

When sending emails 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, etc.) are to be used. 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 kept away from the office should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g. on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. If paperwork has to be taken away from a client's home (e.g. unable to make a required phone call during a home visit) must ensure that it is returned to the client's home on the next visit.

If you are carrying documents relating to a number of clients when on a series of home visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the clients home. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain AUKG's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

Retention of Records

All records should be electronic where appropriate and hard copy documents scanned and attached to the record and the appropriately disposed of. Paper records (where they exists and are not held electronically) should be retained for the following periods at the end of which they should be shredded:

Client records – 6 years after ceasing to be a client.
Colleague records – 6 years after ceasing to be a colleague.
Unsuccessful colleague recruitment documentation – 6 months after vacancy closing date.

Volunteer records – 6 years after ceasing to be a volunteer.
Timesheets and other financial documents – 7 years.
Employer's liability insurance – 40 years.
Other documentation, e.g. information sent to a volunteer as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

Electronic records e.g. Charitylog, to be retained electronically until such time as the individual withdraws consent or the record reaches 40 years in age (this is primarily to allow us to provide input or services to individuals throughout their older age and to ensure their wishes when gifting a legacy are appropriately administered). Supporter records – 6 years after the end of the accounting period the donation / opt-out consent / deceased notification was received. Thereafter, records will be anonymised for reporting purposes.

Artificial Intelligence

Risks:

Using AI platforms involves significant data protection and information governance risks. Including unintentional disclosure and malicious exploitation of sensitive data and compromised data access. It should be assumed that any information shared in AI platforms could be shared with any global user.

Colleagues should be aware that the outputs from Generative AI platforms are prone to significant risks. AI models are trained on vast datasets, but they lack the ability to understand context, nuance, or real-world implications. This can lead to several issues:

- Errors and Misleading Information: AI can generate incorrect or misleading content due to limitations in data quality, biases in training data, or misunderstandings of prompts. For example, AI image generators have produced images of people with extra fingers due to their inability to accurately process visual information.
- Unethical, Biased, or Nonsensical Content: AI models can perpetuate harmful stereotypes or biases present in their training data. Additionally, they may generate content that is irrelevant, incoherent, or even offensive.
- Copyright and Trademark Infringement: AI-generated content can inadvertently incorporate copyrighted or trademarked material without proper attribution.
- Cultural and Social Inappropriateness: AI may generate content that is insensitive to cultural differences or violates social norms.
- Inaccurate Legal Information: AI can provide incorrect legal advice, often based on data from different jurisdictions or outdated laws.
- Inauthentic information being presented: information shared with us, such as CVs may be written by AI and not a true reflection of the writer, their experience, or their views.

Environmental concerns:

When using AI colleagues must be aware of the environmental impact of these activities. Particularly due to the high energy and water consumption required to train and operate large models. These processes contribute to carbon emissions and place additional strain on electricity grids and water resources.

Guidance of use:
Staff, volunteers, and others acting on behalf of Age UK Gloucestershire must adhere to the following guidelines when using Generative AI platforms to help mitigate the risks outlined above:

- Protect People's Privacy: Never input any personal or organisational data or sensitive information into Generative AI tools. This includes names, addresses, health details, financial information, or any data that could identify an individual.
- Protect Confidential Data: Avoid using any confidential or internal Age UK Gloucestershire documents as input.
- Fact-Check Outputs: Always verify any statistics, claims, or information about ageing, benefits, or services for older people generated by Generative AI tools against trusted sources before using them.
- Maintain Age UK Gloucestershire's Voice: Edit AI-generated content to ensure it reflects our tone, values, and expertise in supporting older people. AI should assist, not replace, our unique perspective and experience.
- Avoid Sensitive Topics: Do not use AI to generate content on highly sensitive or complex issues affecting older people, such as end-of-life care or abuse, without expert human oversight.
- Respect Copyright: Ensure any AI-generated content does not infringe on copyrighted materials, especially when creating resources or campaign materials for older people.
- Balanced Use: Consider whether using Generative AI truly improves efficiency for your task. For tasks requiring nuanced understanding of older people's needs, direct human expertise may be more appropriate.
- Follow proper channels for Generative AI tools: Employees interested in acquiring Generative AI

tools from a supplier must follow Age UK Group's procurement policy which requires due diligence and in complex cases a Data Protection Impact Assessment by the IP&C team.

Approved AI Systems:

Many systems are incorporating AI into the products as standard. Use of AI capabilities of the listed systems within this policy is permitted.

To minimise risks listed above all colleagues who use AI should default to Microsoft Co-Pilot where possible rather than more open tools such as Chat GPT. This keeps the information within our environment, reduces risks of information being accessed externally.

In addition to this the cloud based systems listed above have been approved for use of their built in AI functionality.

There will be occasions when Co-Pilot or approved Cloud Based systems cannot carry out the tasks required at which point Age UK Gloucestershire's DPO (CEO) should be consulted prior to use to ensure.

We encourage innovation and our risk appetite for developing AI tools to increase efficiency is open. All development must be discussed with AUKG DPO (CEO) prior to taking place.

What to Do If There Is A Breach

If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Management Team to prevent a reoccurrence. The CEO should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the Board of Trustees. There is a time limit for reporting breaches to ICO so the CEO should be informed without delay.

In the event that the breach involves clients receiving a service commissioned by One Gloucestershire ICB (e.g. Out of Hospital), they should be informed by the Chief Executive or relevant Manager by emailing or by phoning the designated contract manager in the first instance.

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

The Rights of an Individual

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

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).
- Data cannot be used for the purposes of direct correspondence on fundraising or other AUKG services if the Data Subject has declined their consent to do so.

Individuals have a right to have their data erased and to prevent processing in specific circumstances:

- Where data is no longer necessary in relation to the purpose for which it was originally collected.
- When an individual withdraws consent.
- When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

- Personal data was unlawfully processed.

An individual has a right to restrict processing – where processing is restricted, AUKG is permitted to store the personal data but not further process it. AUKG can retain just enough information about the individual to ensure that the restriction is respected in the future. An individual has a 'right to be forgotten'.

AUKG will not undertake direct telephone marketing activities under any circumstances.

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

The CEO will then use the Data Subject Access Request template to keep a record of the request and actions taken. Link to the template is https://ageukgloucestershire.sharepoint.com/:w:/s/Test-Leadership-GDPR/Edme5J5k2A5LmWPqoku2PkQBXLAGfchP6APXhB97UCFYEA?e=ydk02e

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

Further information is available at https://ico.org.uk/

Details of the Information Commissioner

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

Phone: 0303 123 1113

Procedure Addendum: Operational Procedures for Data Protection and Information Governance

This addendum outlines the step-by-step procedures to complement the principles and policies set out in the Data Protection and Information Governance Policy.

Data Breach Reporting Procedure

- Report suspected breaches immediately to your line manager.
- Line manager assesses and escalates to the CEO (DPO) without delay.
- CEO determines if the breach must be reported to the ICO within 72 hours.
- Complete a breach report using the internal template and store securely.
- If commissioned services are affected, notify the relevant contract manager.
- If third party data is involved, notify the third party without delay

Subject Access Request (SAR) Procedure

- SARs must be submitted in writing to the CEO (DPO).
- CEO logs the request using the SAR template and acknowledges receipt.
- Compile relevant data from electronic and paper records.
- Respond within 30 calendar days.
- Securely store all correspondence and disclosures.

Data Sharing Procedure

- Verify consent before sharing personal data externally.
- Check for Data Sharing Agreements
- If consent is unavailable, escalate to the CEO (DPO) for review.

Data Retention and Disposal Procedure

- Regularly review records for disposal eligibility.
- Shred paper records using cross-cut shredders or approved services.
- Securely delete electronic records using certified data erasure tools.
- Log disposal actions with date, record type, and responsible person.

New System or Vendor Onboarding Procedure

- Complete a due diligence checklist for new systems/vendors.
- Conduct a Data Protection Impact Assessment (DPIA).
- Obtain approval from the CEO (DPO).
- Ensure contracts include data protection clauses and security standards. Including statements that data breaches will be reported without delay

Training and Induction Procedure

- All new staff and volunteers complete data protection training at induction.
- Annual refresher training is mandatory or when policies change.
- CEO (DPO) tracks training completion via the Learner Management System (iHasco).

Version History Revision date	Summary of Changes	Other Comments
22 May 2018	Rewritten policy to reflect new GDPR agreed by Mgmt Team	For review in 6 months as GDPR approach implemented.
12 March 2020	Updated following trustee review and office move.	Review in 2 years
20 January 2023	Updated	
16 April 2024	eTapestry data retention policy added	
24 September 2024	Added in link to data request form	
03 September 2025	Updated list of systems and AI section added	
27 October 2025	Procedure addendum incorporated	Review in 2026 following full transition to CSG