DATA PROTECTION POLICY

Update	Version	Author	Date
Policy updated	V1.1	DPO	03.06.2025
Last Review		DPO	June 2026

Age UK Lewisham and Southwark
Registered address: Stones End Centre, 11 Scovell Road, London SE1 1QQ Charity registration number: 296862
ICO registration number: Z533723

1 Scope

Age UK Lewisham and Southwark here after referred to as 'the organisation', a charity registration number Z5337230 with a registered address at Age UK Lewisham and Southwark, Stones End Centre, 11 Scovell Road, London, SE1 1QQi s committed to being fully compliant with all applicable UK and where applicable EU data protection legislation in respect of personal data, as well to safeguarding the rights and freedoms of persons whose information may be processed by Age UK Lewisham and Southwark pursuant to the UK General Data Protection Regulation 2020 (UK GDPR), the Data Protection Act 2018 (DPA) and any other applicable legislation. In this document all such legislation is collectively referred to as 'data protection legislation'.

This policy applies to all employees of the organisation including contractors and subcontractors, and any other persons that are authorised to access the data for which the organisation is the controller.

This policy and procedures should be read in conjunction with the following Age UK Lewisham and Southwark policies:

- ICT policy and Physical Security of Information Policy
- BYOD Offsite Working Policy
- Confidentiality policy
- Safeguarding policy
- CCTV policy
- Subject Access Request Policy
- IG Incident Management Procedure
- IG New Processes Policy and Procedure
- Information Governance Policy
- Data Retention Policy
- Record of Processing Activities
- GDPR and Home Visits Procedure

2 Definitions used in this policy

Data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Data processor: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Data Protection Officer (DPO)*:* DPOs assist an organisation to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO)

Data Protection Lead/accountable person: is the member of the organisation's staff who

oversees data protection obligations and procedures

Data subject: refers to any living person who is the subject of personal data (see above for the definition of 'personal data') held by the organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social

Information Commissioner's Office (ICO)*:* the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

Personal data: means any information that identifies, directly or indirectly, a data subject

Processing: refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise

Special categories of data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership biometric data (where used for identification purposes) data concerning health; data concerning a person's sex life or sexual orientation.

3 The appointment of a Data Protection Officer and a Data Protection Lead

The organisation has assessed the need for Data Protection Officer and has decided that this role should be outsourced to Hope and May Limited who are expert data protection officers specialising in the voluntary sector. Their role is to oversee processing activities and offer impartial advice and guidance to ensure compliance with data protection laws.
A Data Protection Lead has been assigned internally to work with the organisation's DPO and staff to embed good data protection practices. This role is held by the Director of Operations.

4 How personal data may be collected

The organisation collects personal data by various means including but not limited to directly from the individual, from third parties including local authorities, and via the website.
Personal data may be processed using the CRM, it may also be processed by telephone or in person.
Personal data may also be gathered by the use of social media and photography.

5 The seven principles of data protection

Age UK Lewisham and Southwark is committed to adhere to Article 5 of the UK GDPR which lists all the seven principles of data protection:

- **lawfulness, fairness and transparency:** the organisation is committed to process data lawfully, fairly and in a transparent manner
- **purpose limitation**: the organisation collects personal data for specified, explicit and legitimate purposes. the organisation doesn't further process data in a manner that is incompatible with those purposes
- **data minimisation:** the organisation is committed to process data that is adequate, relevant and limited to what is necessary
- **accuracy:** personal data are kept accurate and kept up to date
- **storage limitation:** the organisation is committed to keep personal data for no longer that necessary
- **integrity and confidentiality**: the organisation processes data 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
- **accountability**: the organisation is able to demonstrate compliance by keeping records of processing activities, delivering regular awareness training and keeping a policy framework.

6 Lawfulness, fairness and transparency

6.1 Lawful basis

Age UK Lewisham and Southwark identifies a lawful basis before they processing any personal data. Please see section 5 for more information on the six lawful bases of processing data.

6.2 Privacy notice

Age UK Lewisham and Southwark is committed to informing all data subjects about the processing of their data beforehand so that they are able to make an informed decision about whether or not to provide that data. A Full privacy notice is made available to anyone who wants to know more about how the organisation processes data of the data subjects. The organisation provides shorter statements/easy read version of the privacy notice to specific categories of data subjects, namely:

1. Service users
2. Employees and workers
3. Volunteers and Trustees
4. Any other individuals authorised to process personal data

Age UK Lewisham and Southwark has complied with Art 13 and 14 of the UK GDPR which list the content that needs to be included in the privacy notice and shorter statement.

Unless it would involve disproportionate effort, the organisation will provide the data subject with the privacy notice within a reasonable period but no more than a month from when the data has been obtained. If the data is to be used for communicating with the data subject, the data subject must be informed within the first communication. The organisation may not provide the data subjects with a privacy notice if the data subject already has already received such information by the source of the data.

Age UK Lewisham and Southwark may periodically change how personal data are processed. The organisation will inform the data subjects, accordingly, as required by the data protection legislation

7 Purpose limitation

Age UK Lewisham and Southwark collects personal data for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

The organisation may extend a purpose to cover new processing, as long as the new purpose is compatible with the old. Compatibility is measured according to 'reasonable expectation' the data subject may have. The organisation needs to process information to carry out its work, meet objectives and comply with the contractual obligations of funders. The organisation will only ever collect information that is needed in order to carry out its work, improve its services, report to funders, contract holders and partners and to fulfil any request that data subjects
make, personalise services to best meet data subjects' needs and to keep track of the impact and quality of the organisation work.

The purpose of the data processing is included in the Privacy notice(s) and in the ROPA spreadsheet which is maintained and reviewed regularly. Please see section 4.6 for more information on the RoPAs.

8 Data minimisation and accuracy

Age UK Lewisham and Southwark is committed to the quality of the data that it collects and processes. This means that the data must be:

- adequate
- relevant
- limited to what's necessary
- accurate
- kept up-to-date.

In order to guarantee data quality and compliance, staff members receive clear guidance and training, refresher trainings and briefings during meetings in reference to personal data collection and processing by the Data Protection Officer on an annual basis.

Managers monitor the quality of the data that staff or volunteers record and provide comments in supervisions if standards show any sign of slipping.

The RoPAs spreadsheet (see section 4.6) keeps a log of the personal data processed for each data subject and where that data is stored. This helps to identify staff members who are in charge of updating or deleting data from the different sources of storage.

The organisation carries out annual review of all methods of data collection, checking that they are still appropriate, relevant, and not excessive.

The organisation is aware of the importance of collecting and maintaining accurate personal data. The organisation will assume that information submitted by data subjects is accurate at the date of submission. Data subjects are promptly informed via the privacy notice that they are responsible for ensuring that the personal data held by the organisation is accurate and up to date.

All staff members including Trustees, volunteers and authorised third parties are required to update the organisation as soon as reasonably possible of any changes to personal information, to ensure records are always up to date.

The organisation shall, on an annual basis, carry out a review of all personal data controlled by the organisation and decide whether any data are no longer required to be held for the stated purposes and where required, arrange for that data to be deleted or destroyed in accordance with the requirements of the Data Protection Legislation.

9 Storage limitation

Age UK Lewisham and Southwark will not keep data subjects' data longer than is necessary. When the organisation no longer needs it, it will dispose of the information securely and may use specialist external companies to do this.

In some cases, retention will be based on legal consideration. In other cases, the reason may be more practical or based on organisational decisions. The retention schedule is logged in the RoPAs spreadsheet (see section 4.6) and data subjects are informed via the privacy notice.
Personal data are retained according to the retention scheduled logged in the RoPAs and are destroyed or deleted in a secure manner as soon as the retention date has passed.

Should any personal data be required to be retained beyond the retention period set out in the ROPA, this should be agreed with the accountable person, with consultation with the DPO and should be documented in line with data protection requirements.

10 Integrity and Confidentiality

Age UK Lewisham and Southwark maintains appropriate technical and organisational measures to protect personal data from unauthorised access, loss, or misuse. Access to personal data is restricted to authorised personnel only. In exceptional cases, personal data may be disclosed to third parties such as law enforcement agencies where required by law or in the vital interests of the individual."

The organisation limits access to the data only to those employees, contractors and agents who need such access in connection with providing products or services to data subjects, or for other legitimate purposes.

The organisation will ensure it delivers regular data protection training to its employees, trainees, volunteers and freelancers about its data protection practices. Records are maintained.

All employees of the organisation are responsible for keeping secure any personal data

controlled by the organisation. Under no circumstances may any personal data be disclosed to any third party unless the organisation has provided express authorisation or has entered into a

confidentiality agreement, a data processor agreement, or a data sharing agreement with the third party (see section 8. Such agreements should include the lawful basis for sharing the data for allowing access to the personal data.

Security measures

There are several physical security measures that Age UK Lewisham & Southwark puts in place, including (but not limited to):

20.5.1 clear desk policy to avoid people leaving confidential data on their desk
20.5.2 locked filing cabinets, drawers or lockers for confidential paperwork
20.5.3 automatic screen shut down when staff members are away from their desk
20.5.4 arrangements for shredding paper
20.5.5 manual records which have passed their retention date must be shredded and disposed of as 'confidential waste'

Confidentiality

Age UK Lewisham and Southwark operates under a policy of confidentiality. Age UK Lewisham and Southwark is committed to providing confidential services to their stakeholders, and ensuring that all personal data about staff, trustees, volunteers and other stakeholders are treated as confidential, and collected, processed and retained in line with the data protection law. In certain situations, information may need to be shared with third parties, for example to protect the welfare and safety of our users who receive help and support which is part of the service delivery. Please see the **Confidentiality Policy.**

11 Accountability - demonstrating Compliance

In accordance with law requirements, the organisation keeps records that they can demonstrate the steps taken to comply with UK GDPR:

- **Record of Processing Activities (RoPAs) spreadsheet** identifies information such as the category of persona data processed for each data subject, the lawful basis of the processing, data retention, data storage, who is responsible for the data and who has access to the data
- **The Activity, Incident and Risk reporting spreadsheet** keeps a log of key information such as discussions and decisions about data protection, identified risks, any personal data breaches and response, training of staff and volunteers, requests to exercise any rights by data subjects and

management of those requests, notifications to the ICO

- **Legitimate interest assessments** (LIA) that have been carried out (see section 5.4 for more information)

- **Data protection impact assessments** (DPIA) that have been carried out to justify the approach where processing poses particular risks (such as processing of special category of data) – see section 7.3 for more information
- **Data protection policy** which includes most procedures relating to data protection
- **Privacy notice** for data subjects (see section 4.1.2)
- **Processors agreements** with database, CRM and cloud providers and other data processors (see section 8 for more information)
- **Data sharing agreements** (also called information sharing protocol) with other data controllers or joint controllers (see section 8 for more information)
- **Appropriate Policy Document (APD)** which may be completed in some circumstances outlined by the DPA (2018) when processing special category of data or criminal records

12 The six lawful bases for processing personal data (including special category data)

Age UK Lewisham and Southwark processes personal data by identifying a 'lawful bases' chosen from the six possibilities set out in Article 6 of the UK GDPR:

a. with consent of the data subject
b. for a contract involving the data subject (where a consideration is received)
c. to meet a legal obligation (where a law requires the data to be processed
d. to protect any personal vital interests (where the data subjects' life depends upon our processing of their data.
e. in the organisation's legitimate interests provided the data subject's interests are respected
f. in the public interest (May provide the ability to process special category data where this is used as the secondary bases in conjunction with an article 6 condition)

The most common lawful basis that the organisation identifies are legitimate interest and consent (Please see section 5.1 of the policy), contract, legal obligation and legitimate interest. The lawful bases for the different processing activities are recorded in the Record of Processing Activities (RoPAs) spreadsheet which is maintained and reviewed regularly.

When data processing poses particular risks (such as the processing of special category data (see

section *7.3 Risk Assessment* for more details)), the organisation will complete a Data Protection Impact Assessment (DPIA) to justify the data protection approach.

When processing special categories of data or criminal records (see section 6) without the consent of the data subject, data protection law requires to identify another lawful basis under Art 6 of the UK GDPR other than consent, supported by one of the conditions of Art 9(2) which may require the support of a conditions listed in schedule 1 and 2 of the DPA 2018. For the avoidance of doubt, when processing criminal records, including DBS checks, the lawful basis identified in article 6 and article 9 of the UK GDPR needs to be additionally supported by the DPA (2018).

The organisation may complete an Appropriate Policy Document (APD) for the processing of special categories of data and criminal data without consent of the data subjects as required by law.

13 *Consent*

Where Age UK Lewisham and Southwark chooses consent as its 'lawful basis', it means that the data subject has given their consent to the processing of their personal data for one or more specific purposes. The organisation will gather a proof of that consent in order to demonstrate that the data subject has consented to processing of their personal data (as per Article 7.1 of the UK GDPR). The data subject still has the right to withdraw their consent at any time (as per Article 7.3 of the GDPR). Please see section 7.2 for more information on data subject's rights.

Consent to the processing of personal data by the data subject must be

- Explicit - demonstrated by active communication between the data controller and the data subject and must not be inferred or implied by omission or a lack of response.
- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information
- Specific and informed (it should cover the controller's name; the purposes of the processing and they types of processing activities)
- A clear and unambiguous indication of the wishes of the data subject
- In relation to sensitive data, consent may be provided in writing, if given verbally must be acknowledged in writing.

The organisation understands that Consent is for the time being and may review and refresh

consent as appropriate.

Consent will not be the condition for processing data where a service or product is purchased.

13.1 Consent and minors

The organisation may gather consent directly from minors if they are 16 or older.

If the organisation supports a young person under 16, the organisation may:

20.5.1 gather consent from a parent, carer, or guardian

20.5.2 gather consent from a local authority that acquired parental responsibility when the minor is made subject to a care order by the court

20.5.3 gather the young person consent subsequently to an assessment of competence made and documented by a relevant staff member

A young person's consent may override consent gathered from their parents or carers.

14 Contract

The organisation identifies contract as its lawful basis when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.

15 Legal obligation

The organisation identifies legal obligation as a lawful basis when processing is necessary for compliance with a legal obligation to which the controller is subject.

16 Legitimate interest

Where the organisation chooses legitimate interest as its lawful basis, a Legitimate Interest assessment may be completed in order to show what Age UK Lewisham and Southwark's interest is and that it is legitimate, to show why the processing is necessary in pursuing this interest, to consider potential impact on any data subjects' rights and freedom and to measure whether the data subject might reasonably expect us to process their data. An opt-out option may be made available to the data subject. Data subjects always have a right to object to the processing of their data. This condition is the primary condition for processing personal data including special

categories of data as mentioned above. Where such data is processed, an appropriate policy document will be relied upon.

17 Data subjects and data specifications

The organisation collects personal information from different groups of data subjects:

- Service user
- Third parties including carers
- volunteers
- job applicants
- web and social media data subjects
- attendees of events
- freelancers
- donors
- employees
- trustees

Our privacy notice and RoPAs will explain the different kinds of data we collect and the lawful basis for processing this. We process normal category of data, and we may also collect special categories data and criminal data.

Criminal records are not formally special category data, however, under the Data Protection Act 2018, criminal records data receive the same additional protection as special category data.

For more information on how we process special categories of data and criminal records, please section 5.5.

The RoPAs spreadsheet (section 4.6) keeps a record of the data specifications that the organisation collects for each data subject.

18 Additional compliance obligations

Age UK Lewisham and Southwark is committed to comply with the additional obligations in reference to the UK GDPR and the Data Protection Act 2018. These include:

a. breach notification

b. data subject's rights
c. risk assessment
d. by design and by default
e. Data controller fees payments

19 Breach notification procedures

Article 4.12 of the UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

These are the steps taken by the organisation in case of a data breach:

- Any staff member who discovers a personal data breach is required to immediately inform their line manager and the DPO.
- The staff member and/or their line manager need to ensure that the breach is not still occurring and take any immediate mitigating action that may reduce the impact of the breach, at the advice of the DPO.
- In conjunction with Article 33.1 of the UK GDPR, the DPO, on behalf of the organisation must report the data breach to the ICO within 72 hours 'unless the personal data breach is unlikely to result in a risk to the rights and freedom of natural persons'. The decision to report such a breach will be made by the organisation on advice of the DPO.
- If the breach is reportable, the DPO will make the report using the ICO's website. Factors that may determine whether a breach is reportable include:
  - sensitivity of the categories of data. For example, data identifying a health condition
  - quantity of data concerned
  - whether there is a potential for a high risk of harm to the data subjects concerned

  Mitigating factors that may be considered when not reporting a breach:
  - the data is retrievable
  - evidence that data has been contained and that those who may have access will not process the data in such a way as to cause harm or distress to the data subjects concerned.
- If the data breach is reported to the ICO, the organisation will make available any documents or records that the ICO requires to peruse the inquires. The organisation will cooperate with the ICO with any request and record any guidance the ICO gives in accordance with the breach in the activity incident and risk reporting spreadsheet (please see section 4.6 for more information on this spreadsheet).
- If the data breach is likely to result in a high risk to the rights and freedoms of natural persons (e.g.,

where the breach could result in ID theft or fraud; physical harm; significant humiliation and/or damage to reputation) the organisation would need to communicate the breach of their personal data without undue delay to the affected individuals. In some circumstances, the organisation may decide to not inform the individuals if by doing so it would cause more damage and anxiety to the data subjects than the data breach itself.

- If the individuals are informed of the data breach, the organisation will also ask if they want to log a formal complaint to the ICO for how their personal data has been managed.
- The data breach is then logged into the activity incident and risk reporting spreadsheet in order to identify lessons the organisation can learn and the changes that can be made. If the data breach is reported to the ICO, the case number supplied by the ICO will be recorded in the activity incident and risk reporting spreadsheet.
- Train staff where required to ensure the breach doesn't happen again.

The agreements that the organisation stipulates with data processers include a clause requiring them to inform the organisation immediately or in any event within 24 hours of them becoming aware of a breach. This is to allow the organisation to make a report to the ICO within the 72 hours.

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation.

Contractors, subcontractors, and other parties may be subject to appropriate legal action in accordance with the organisation's processor agreement. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred immediately to the relevant authorities.

20 Data subjects' rights

Age UK Lewisham and Southwark is fully aware of the data subject rights described in Articles 15 to 22 of the UK GDPR and these are listed in the privacy notice.
The data subjects' rights include:

1. The right to be informed
2. The right of access
3. the right of rectification
4. the right to be forgotten (erasure)

5. the right to restrict processing
6. the right to data portability
7. the right to object processing
8. rights in relation to automated decision making and profiling

Additional rights of the data subjects:

- the right not to receive direct marketing
- the right to claim damages should they suffer any loss as a result of a breach of the provisions of the UK GDPR
- the right to complain - right to request that the ICO carry out an assessment

If data subjects wish to exercise any rights, they can contact the organisation at data.protection@ageuklands.org.uk, 020 7701 9700, or they can write to us Stones End Day Centre, 11 Scovell Road, London, SE1 1QQ. They are reminded of their rights and how to exercise them in the privacy notice they receive (see section 4.1.2)

All staff members are trained to recognise an incoming request to exercise any right, to understand when the right applies and to pass in on without delay to the designated person.

All requests from data subjects to exercise any rights are recorded into the Activity, Incident and Risk reporting spreadsheet (please see section 4.6 for more information on this spreadsheet).

Under certain circumstances, mostly described in Schedules 2-4 of the DPA (2018), the organisation may not need to comply with the request by a data subject to exercise one of their rights. Those circumstances will be assessed on a case-by-case basis.

20.1 The right to be informed

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The organisation is committed to comply with this right and they do so via the privacy notice (see section 4.1.2).

20.2 The right of access and SAR procedure

A data subject has the right to make access requests in respect of personal data that is held and disclosed. To understand how we deal with Subject Access Requests, please view our **Subject**

20.3 The right of rectification

Age UK Lewisham and Southwark is aware of the provisions in Article 16 of the UK GDPR: if the data subject becomes aware that the organisation is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

In conjunction with Article 19 of the UK GDPR, the organisation informs of the right exercised by the data subject to anyone to whom data have been disclosed, unless this 'proves impossible or involves disproportionate effort'. Age UK Lewisham and Southwark will also inform the data subject which recipients' data have been disclosed to, if they ask.

20.4 The right to be forgotten (erasure)

If a data subject asks the organisation to delete their information, as stated in Article 17, the organisation will do so without undue delay when:

a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.
b) the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing.
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing.
d) the personal data has been unlawfully processed.
e) the personal data has to be erased for compliance with a legal obligation.

In addition, if the organisation has made the information public, the organisation must try to get it erased in other locations as well. In conjunction with Article 19 of the UK GDPR, the organisation informs anyone to whom data have been disclosed, unless this 'proves impossible or involves disproportionate effort'. The organisation may also inform the data subject to which recipients their data have been disclosed.

There are exceptions to the 'right to be forgotten' for reasons relating to freedom of expression, public interest, archiving, research and statistics, legal claims and legal obligation.

There may also be circumstances where the organisation has no choice but to retain data, for example to mark a record for suppression in order to ensure that no direct marketing is sent to that individual in the future.

The organisation will process a request for erasure without undue delay and normally within one month.

20.5 The right to restrict processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following

applies:

20.5.1 the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data

20.5.2 the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead

20.5.3 the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims

20.5.4 the data subject has objected to processing pursuant to Article 21(1) of the UK GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

20.6 The right to data portability

This right applies when processing is based on consent or a contract between the organisation and the data subject and the process and the processing is taking place 'by automated means'. It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Data subjects are entitled to receive from the organisation a copy of any personal data they have provided, in a 'structure, commonly used and machine-readable format', so that they can provide the data to a different controller.

20.7 The right to object processing

Data subjects can object to any processing of their data that organisation is carrying out on the lawful basis of legitimate interests. The organisation will stop processing if not able to demonstrate

a ‘compelling legitimate reason’.

20.8 Rights in relation to automated decision making and profiling

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. Profiling refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject’s employment performance, economic status, whereabouts, health, personal preferences and behaviour.

The data subject has the right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling. The data subject has the right not to have decisions made about them solely by automated processing if this has a significant effect on them, unless the decision is necessary in conjunction with a contract between the data subject in the controller or the data subject has provided an explicit consent.

Age UK Lewisham and Southwark does not currently undertake automated decision making.

20.9 The right not to receive direct marketing

Every data subject has the right not to receive direct marketing if that is their choice Means to Opt-out are available and signposted within correspondence and an explanation of this can on the website.

20.10 The right to claim damages in case of data breach

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation. See section 7.1 for more information about data breach.

20.11 The right to complain

If data subjects wish to make a complaint or share concern, they should be firstly encouraged to liaise directly with the organisation. They can make a complaint or send an email to data.protection@ageuklands.org.uk, who will respond within 5 working days and lead on the resolution of the complaint within 28 days.

As stated in the privacy notice, the organisation will inform the data subject that can also make a complaint to the ICO and request that the ICO carries out an assessment as to whether any of the

provisions of the UK GDPR have been breached. Data subjects can remain anonymous if they wish.

21 *Risk Assessment*

Risk Assessment is an important part of the accountability of an organisation. It is vital that the organisation is aware of all risks associated with personal data processing and it is via its risk assessment process that the organisation is able to assess the level of risk.

It is the policy of the organisation not to transfer or sharing data into an environment that is not considered compliant with UK data protection law

In addition to this, where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the rights and freedoms of natural persons, the organisation is required to engage in a risk assessment of the potential impact, also known as a 'Data Protection Impact Assessment' (DPIA). More than one risk may be addressed in a single DPIA. The organisation has developed and agreed upon a procedure for completing a DPIA. This procedure is always followed where there is a need to measure risk. The procedure is completed by the Data Protection Lead and if necessary, the opinion of a professional Data Protection Practitioner is taken into account.

If a Data Protection Impact Assessment (DPIA) identifies that a planned activity is likely to result in a high risk to the rights and freedoms of data subjects including risks of physical, emotional, or psychological harm the matter must be escalated to the Data Protection Lead and, where relevant, the Safeguarding Lead. If such risks cannot be mitigated, the organisation will consult the Information Commissioner's Office (ICO) before proceeding in accordance with Article 36 of the UK GDPR."

22 *By design and by default*

This policy includes procedures in relation to data protection across the organisation, involving different staff members, teams and delivery. As the organisation aims towards full compliance

Age UK Lewisham and Southwark remains responsible for what happens to the data and remains liable for any mistakes of the data processors. In the contract with the data processor, Age UK Lewisham and Southwark may include a provision that requires the data processor to reimburse Age UK Lewisham and Southwark.

and therefore also towards a data protection "by design and by default", these procedures will be embedded into the operating guidance as appropriate.

The goal of this principle would mean that in the organisation, everyone who starts a new project or sets up a system or a process must ensure that they incorporate data protection as a matter of course, consulting the Data Protection Lead. Consideration of the data protection implications should be a standard check point before any project or system is signed off.

23 Registration to the ICO and fees

The organisation has registered with the Information Commissioner as it engages in the processing of personal information identifying data subjects directly or indirectly.

The organisation pays an annual fee to ICO, as required by law. The data controller registration number for Age UK Lewisham and Southwark is Z5337230 and annually renews on the 18th July.

24 Data sharing - working with other organisations

As any other organisation, Age UK Lewisham and Southwark may collaborate with:

- data processors
- joint controllers
- separate controllers

All third parties we work with who have or may have access to personal data of our data subjects, will either comply with this policy, or we will ensure that their data protection policy aligns with this

policy.

25 Data Processors

A data processor is a company or organisation, or an individual who is not an employee or volunteer, that processes data on behalf of the data controller (Age UK Lewisham and Southwark in this policy).

Before deciding to use a particular service, the organisation would check the terms and conditions and decide whether it is compliant before deciding to use that service.

With freelancers, external researchers and IT companies, the organisation stipulates a Processor Agreement or a contract including data protection provisions, as outlined by Article 28.3 of the UK GDPR.

26 Joint Controllers

Art 26 of the UK GDPR, define *joint controllers* as two or more data controllers which jointly determine the purpose and means of processing. When Age UK Lewisham and Southwark collaborates with a data controller, the parties must agree to a Joint Controller Agreement which could include the following:

- who it applies to
- general data protection principles, including the basic principle of confidentiality
- the purposes for which information will be shared
- the lawful basis on which sharing will take place
- how each partner will discharge their transparency obligations, and whether all parties will use the same form of words to ensure consistency
- procedures for sharing information, and in particular for obtaining and recording consent from the data subject (if this is the lawful basis)
- procedures to ensure that all parties have the same understanding of how to comply with the data protection principles regarding data quality and retention
- access and security procedures
- procedures for ensuring that the handling of data subjects' rights is consistent and fully compliant
- procedures for raising concerns or resolving difficulties
- how the agreement will be managed and kept under review?

The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the privacy notice for those data subjects affected by the data sharing and the collaboration between the organisation and the joint controller.

27 Separate Controller

The organisation may collaborate with another organisation which is a separate controller as information are merely disclosed to one other. In this case, the organisation may agree to a Data Sharing Agreement with the other separate controller(s), which defines the following:

- parties involved in the agreement
- purpose for which information will be shared
- the lawful basis on which the sharing will take place
- other organisations involved in the data sharing
- what data items will be shared (including special category of data)
- procedures to comply with data subjects' rights
- governance arrangements

The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the Privacy notice for those data subjects affected by the data sharing and the collaboration between the organisation and the other separate controller(s).

28 International Data Transfer

Where personal data are stored outside of the UK, safeguards to protect personal data may include but are not limited to the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs). Transfers will be assessed on a case-by-case basis.

29. National Data Opt-Out Policy

Age UK Lands acknowledges the NHS National Data Opt-Out policy, which allows individuals to opt out of their confidential patient information being used for purposes beyond their individual care (such as

planning and research). At present, the organisation does not engage in any data sharing activities that fall within the scope of the National Data Opt-Out, a nd therefore is not required to apply opt-out filtering to data disclosures. However, we are committed to reviewing our data processing activities periodically to ensure continued alignment with national guidance.Should our data use change in the future to involve purposes covered by the National Data Opt-Out, appropriate technical and procedural measures will be put in place to ensure full compliance.

30. Changes to this policy

This Policy is updated regularly by the Data Protection Officer when required. It is reviewed annually by the Senior Management and the Board of Trustees.

LAWFUL BASIS RELIED ON BY AUKLS			
PURPOSE/ACTIVITY	**LEGAL BASIS UNDER ARTICLE 6 UK GDPR**	**LAWFUL BASIS FOR SPECIAL CATEGORY DATA UNDER ARTICLE 9 UK GDPR**	**NOTES**
Delivering core services to clients	Legitimate interests	2. Disability support: Substantial Public Interest, read with Schedule 1, Part 2, Condition 16 (disability support) and Condition 17 – counselling	Must be supported by an Appropriate Policy Document (APD)
Supporting vulnerable adults or adults at risk	Legitimate interests	Substantial public interest – safeguarding (Art. 9(2)(g)) + DPA 2018 Sch. 1, para 18 and 19	
Managing employees and payroll	Contract (Art. 6(1)(b)) + Legal obligation (Art. 6(1)(c))	NA	Avoid using consent for staff. Use legal obligation (e.g. for payroll, pensions)
Health information on employees	Legitimate Interest	Health or social care, read with Schedule 1 Part 1, Condition 2	
Fundraising and donor communications	Consent for Text and Emails and Legitimate interests for post or call	NA	Must conduct a Legitimate Interest Assessment (LIA) where relying on LI and provide opt-out; make record of consent and respect withdrawal of consent

Volunteer recruitment	Legitimate interests (Art. 6(1)(f))	Criminal offence data if DBS involved (Art. 10) + DPA 2018 Sch. 1, para 1 or 18	APD required for criminal offence data (e.g. DBS checks)
Data analytics or service improvement	Legitimate interests (Art. 6(1)(f))	Anonymised data preferred	Must not undermine rights and freedoms; a DPIA may be advisable


Lewisham
& Southwark
age UK