Policy no: 4005	Data Protection policy

.

AGE UK CROYDON is an equal opportunities employer and any discrimination or harassment on the grounds of colour, sex, race, nationality, religion, ethnic origin, sexual orientation, disability, marital status, domestic circumstances, trade union membership/non-membership, or age will not be tolerated.

Age UK CROYDON staff, volunteers and Trustees are responsible and accountable for working within the framework of our policies and procedures.

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our clients, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data Users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

2.2 The types of personal data that AGE UK CROYDON (AUKC) may be required to handle includes information about current, past, and prospective suppliers, clients, staff, volunteers and others that we communicate with.

2.3 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.5 This policy has been approved by AUKC's BOARD OF DIRECTORS. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.6 We employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. The Data Protection Officer is responsible

for ensuring compliance with the Act and the HR & Governance lead with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer by emailing DPO@ageukcroydon.org.uk.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 Data is information which is stored electronically, on a computer, or in paper-based filing systems.

3.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. AUKC are the data controller of all personal data used in our business for our own commercial purposes.

3.5 Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on AUKC's behalf.

3.6 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.7 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5.3 Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of our business, we may collect and process the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2 We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

3.1 If we collect personal data directly from data subjects, we will inform them about:

a) The purpose or purposes for which we intend to process that personal data.

b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

3.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, in line with our Data Retention Policy.

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

We will process all personal data in line with data subjects' rights, in particular their right to:

a) The right to be informed

b) The right of access

c) The right to rectification

d) The right to erasure

e) The right to restrict processing

f) The right to data portability

g) The right to object

h) Rights in relation to automated decision making and profiling.

11.1 In order to best meet our client's needs, AUKC will keep accurate records of our professional relationship with our client and may at times wish to share information with other agencies or persons. We will not do either of these without the consent of our client unless otherwise directed under the Data Protection Act:

a. To protect a person's vital interest
b. In order to comply with a court order
c. To fulfil a legal duty, statutory function or legitimate interest
d. To support a statutory function e.g. emergency services

11.2 AUKC will always assume capacity for a person's consent to be valid they must be:

11.2.1 Capable of giving consent (competent)

11.2.2 Have sufficient information to make an informed decision

11.2.3 Act voluntarily (not under any pressure or duress from anyone)

11.3 In situations where the client is unable to make a decision or give consent, AUKC will act according to the "best interests" procedures as laid down in the Mental Capacity Act, recognising that capacity may:

11.3.1 vary

11.3.2 be time specific.

11.3.3 differ for each individual decision.

11.4 AUKC recognises that seeking consent is part of a respectful relationship and should be seen as a process, not a one-off event.

11.4.1 Consent will be sought at the earliest opportunity in a working relationship and should be done in conjunction with an explanation of the Confidentiality policy

11.5 Consent can be Expressed or Implied

11.5.1 All consent must be recorded

11.5.2 Implied consent– Information given voluntarily by the client, but this can't be used for special category data like Ethnicity or Health information. Explicit consent is needed for each use of information.

11.6 Consent will continue to be sought wherever possible or necessary and may include:

11.6.1 Updating case notes with significant changes

11.6.2 Updating computer records and databases with significant changes

11.7 Consent may be given verbally but should be confirmed in writing where appropriate.

11.8 Wherever AUKC needs to contact a third party/agency for explicit personal information or refer client to a third party then written consent should be collected and recorded on the database where possible and practicable.

12. DATA SECURITY

12.1 AUKC will process all personal data we hold in accordance with our Data Security Policy. AUKC will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 AUKC will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they puts in place adequate measures themselves.

12.3 AUKC will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.

b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the database and within the cloud based central Microsoft 365 system instead of individual PCs.

12.4 Security procedures include:

a. Entry controls. Any stranger seen in entry-controlled areas should be reported.

b. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. Methods of disposal. Paper documents should be confidentially shredded. Digital data is anonymised in accordance with our Data Retention Policy.
d. Equipment.

13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

13.1 AUKC may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

a. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
b. The data subject has given their consent.
c. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
d. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
e. The transfer is authorised by the relevant data protection authority where AUKC have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2 Subject to the requirements in clause 12.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

14.2 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, clients, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.3 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

15. DEALING WITH SUBJECT ACCESS REQUESTS

15.1 All individuals have the right to access any information that AUKC holds on them. When an individual makes a request to access the information we hold on them, this is called a Subject Access Request

15.2 Subject access requests can be made to anyone within the organisation and can be

made in any format, including in person, via social media or by email. Organisations have 30 calendar days to respond to valid Subject Access Requests and they must be provided free of charge, unless the request can be deemed as "excessive or manifestly unfounded". Before any information is provided, the IG Lead will verify the identity of the person making the request. For further information, see the Subject Access Request Procedure.

16. RETENTION SCHEDULE

For clients that have not been in contact with AUKC for over two years, only minimal personal information will be kept. Data related to their interaction with any projects will be preserved online, with any personal identifiable information permanently anonymised. This allows Age UK Croydon to continue reporting on project activity without risking personal identifiable data.

Employee records will be kept for 6 years after employment ceases. Financial records relating to sales invoices will be kept for 6 years from the date of the invoice. Volunteer records will be kept for 2 years after engagement completed. Work experience records will be kept for a year after engagement. For clients that have received advice, including financial advice and advice with casework, records will be kept for 6 years. In any case the lawful basis schedule should be referred to for retention periods.

17. ALL NEW AND EXISTING STAFF, VOLUNTEERS AND TRUSTEES WILL AGREE AND SIGN THE INTERNAL DATA PROTECTION POLICY.

18. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or e-mail.

Date this policy came into effect approved by Senior Information Risk Owner	Signature: Name: Sanjay Gulati Date:20 /04/ 2022
Next Review Date	Date: 20 April 2023
Name or position of person responsible for this policy	Signature: *J Francis* Name: J Francis Position: Operations Administrator

Other related policies	Data Security Data Retention Schedule