DATA PROTECTION POLICY AND PROCEDURE

Age UK Enfield is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR), Data Protection Act 2018 and any successor legislation (together, the 'data protection legislation'). Age UK Enfield is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data and special category personal data.

Current Version: 3

Approved by:

Approval date: September 2023

Next review date: September 2025

Version History:

Version	Date	Main Changes	Changed by
1	5/2018	First Issue	
2	9/2020	Second Issue	Silvia Schehrer
2.1	5/2021	Formatting only	Ben Ingber
3	28/09/2023	Update to ICO officer and review	Netta Hunt

Related Documents:

- Privacy Notice
- Confidentiality Policy
- Data Retention Policy including the records retention list
- Privacy Impact Assessment
- Subject Access request

Statement of policy

Age UK Enfield is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR), Data Protection Act 2018 and any successor legislation (together, the 'data protection legislation'). Age UK Enfield is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data and special category personal data.

Age UK Enfield will therefore follow procedures which aim to ensure that all employees and volunteers, and others who have access to any personal data held by or on behalf of the local office, are fully aware of and responsible for the handling of personal data in line with the data protection legislation.

In order to operate efficiently, Age UK Enfield has to collect and use information about people with whom it works. These may include current, past and prospective clients; current, past and prospective employees; current, past and prospective volunteers; and our suppliers.

Age UK Enfield is a Data Controller and has a statutory duty to register with the Information Commissioner. This means that Age UK Enfield has a statutory right to store data about individuals.

The policy applies to all employees, volunteers, trustees, of Age UK Enfield. This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sexual orientation, race, ethnic origin, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data protection legislation and in particular Article 5 (1) of the GDPR requires that personal data shall be used in accordance with the following principles:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5 (2) of the GDPR requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Lawful basis for processing personal data under the data protection legislation

Age UK Enfield process personal data under the following lawful bases:

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Lawful basis for processing special category personal data

Age UK Enfield process special category personal data under the following lawful bases:

Explicit consent: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

Handling of personal data and special category personal data

Age UK Enfield will, through appropriate management and the use of appropriate controls adhere to the following in regards to our use of personal data and special category personal data;

- Provide up to data privacy notices to data subjects.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Ensure the quality and accuracy of information when collected or received and during its use.
- Apply checks to determine the length of time information is retained.
- Take appropriate technical and organisational security measures based on risks to data subjects.
- Not transfer outside the EEA without suitable safeguards.
- Ensure that any information incidents are reported where appropriate the data subject and the Information Commissioners Office.
- Mitigate risks to the data subjects in the event of an information incident using an appropriate data breach policy.
- Ensure that the rights of our data subjects can be properly exercised.

These rights include:

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

In addition, we will ensure that:

- There is someone with specific responsibility for data protection in the organisation. The post responsible for data protection is Information Security Lead.

- Organisational information and in particular privacy risks are risk assessed, documented and controlled.
- Everyone managing and handling personal data and special category personal data understands that they are responsible for following good Information Governance / Assurance practice and for complying with the data protection legislation.
- Everyone managing and handling personal data and special category personal data is appropriately trained and supervised to do so.
- Queries about processing personal data and special category personal data are promptly and courteously dealt with within the requirements of the data protection legislation.
- Data sharing and processing is carried out under an appropriate written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

Consent

Age UK Enfield must record clients' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data cover information relating to:

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

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

As a general rule Age UK Enfield 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 Services/Project Manager or Chief Executive for advice.

Obtaining Consent

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

- 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 from a client in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing were to be undertaken.

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 either in an email or on a computerised record (e.g. Charitylog). The verbal consent is to be recorded in the appropriate fields on the computer 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 Age UK Enfield then the member of staff should discuss this with their manager at the earliest opportunity.

Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc.). The communication may be in any of a variety of formats including mail and email. The responses should be recorded to

inform the next communication. Age UK Enfield will not share or sell its database(s) with outside organisations.

Age UK Enfield holds information on our staff, volunteers, clients and other supporters, to whom we will from time to time send copies of our newsletters, magazine and details of other activities that may be of interest to them. Specific consent to contact will be sought from our staff, clients and other supporters, including which formats they prefer (eg mail, email, phone etc) before making any communications.

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

Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing 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

Age UK Enfield Privacy Statement will also be published on our website.

Types of Data held

We keep several categories of personal data on our employees and clients in order to carry out effective and efficient processes. We keep this data electronically, in a personnel file or care plans relating to each employee and service user and we also hold the data within our CRM and computer systems.

Employee, and Client Rights

You have the following rights in relation to the personal data we hold on you:

a. the right to be informed about the data we hold on you and what we do with it;

b. the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests.

c. the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';

d. the right to have data deleted in certain circumstances. This is also known as 'erasure';

e. the right to restrict the processing of the data;

f. the right to transfer the data we hold on you to another party. This is also known as 'portability';

g. the right to object to the inclusion of any information;

h. the right to regulate any automated decision-making and profiling of personal data.

Responsibilities

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

Lawful Basis of Processing

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee's or clients consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees and clients will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

Access to Data

As stated above, employees and clients have a right to access the personal data that we hold on them. To exercise this right, employees and clients should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be

provided to parties other than the employee or client making the request. In these circumstances, a reasonable charge will be applied.

Data Disclosures

The Company may be required to disclose certain data/information. The circumstances leading to such disclosures include:

a. any employee benefits operated by third parties;

b. disabled individuals - whether any reasonable adjustments are required to assist them at work;

c. individuals' health data - to comply with health and safety or occupational health obligations towards the employee;

d. for Statutory Sick Pay purposes;

e. HR management and administration - to consider how an individual's health affects his or her ability to do their job;

f. the smooth operation of any employee insurance policies or pension plans;

g. to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security

Age UK Enfield have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

In the main data is to be stored on secure electronic cloud-based Customer Relationship Management (CRM) systems e.g. Charitylog and StaffPlan.

When commissioning cloud-based systems, Age UK Enfield will satisfy themselves as to the compliance of data protection principles and robustness of the cloud-based providers.

All necessary members of staff, secondee's, volunteers and Trustees are provided with their own secure login and password, and every IT system regularly prompts users to change their password.

Staff may not use personal (i.e. not supplied by Age UK Enfield) IT systems for Age UK Enfield purposes, including accessing Age UK Enfield email accounts, CRM systems and downloading documents.

All necessary Trustees will be given access to relevant Age UK Enfield documents via secure remote access; these documents must be downloaded or printed only as necessary; any hard copies of these documents must be brought to the relevant Age UK Enfield offices for secure disposal once no longer required. Electronic copies must be securely deleted from

any private IT systems including any metadata relating to the document. Emails containing personal data will be deleted once no longer required for the initial purpose.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of Age UK Enfield containing sensitive information are supervised at all times.

The physical security of Age UK Enfield's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Electronic/Digital Records

With consent client data is stored on a secure electronic, cloud-based, CRM; called Charitylog, or the organisations server.

Staff, secondee, volunteer and organisational data is stored on a secure electronic, cloud-based, CRM system; called CharityLog, or StaffPlan or the organisation's server.

Data should only be stored on the server or cloud-based systems and not on individual computers.

Digital data is coded, encrypted or password-protected, on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be password-protected and kept in an appropriate lockable cupboard or cabinet when not in use.

Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient or the data shared is suitably pseudonymised e.g. Charitylog numbers are used to identify the client.

When sending confidential information, staff will always check that the recipient is correct before sending.

Before sharing data, all staff members will ensure:

- they are allowed to share it
- that adequate security is in place to protect it
- that whoever the data is being shared with has been clearly outlined

Circular emails are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

Where electronic records are taken off the premises, staff will take extra care to follow the same procedures for security.

The person taking the information from the premises accepts full responsibility for the security of the data.

When working off-site, all data protection and confidentiality principles still apply.

Data is never left unattended and/or in clear view during the working the day.

Paper Records

Confidential paper records are kept in an appropriate lockable cupboard or cabinet when not in use, with restricted access.

Workstations should operate a clear desk policy so that any confidential paper records will not be left unattended or in clear view anywhere with general access.

Where confidential paper records are taken off the premises, staff will take extra care to follow the same procedures for security and ensure that lockable crates are used to secure paper records in transit.

The person taking the information from the premises accepts full responsibility for the security of the data.

Any paper records that are no longer required (including 'scrap paper' that contains personal data) must be shredded and disposed of appropriately.

When working off-site, all data protection and confidentiality principles still apply.

Data is never left unattended and/or in clear view during the working the day.

Retention of Records

The details about how long records should be retained are outlined in the organisation's Data Retention policy and schedule.

Third Party Processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain Age UK Enfield's commitment to protecting data.

International Data Transfers

Age UK Enfield does not transfer personal data to any recipients outside of the EEA.

Requirement to Notify Breaches

If you discover, or suspect a data protection breach you should report this to your line manager who will review the systems, in conjunction with the senior management team. All data breaches will be recorded on our Data Breach Register. Where legally required, we will

report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

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

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller officer for Age UK Enfield are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of the Age UK Enfield's policies and procedures.

Records

Age UK Enfield keeps records of its processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Data Protection Compliance

Our registration reference with the ICO is: Z5082844.

Our Information Governance lead is: Peter Glass

Age UK Enfield, John Jackson Library, 35 Agricola Place, Bush Hill Park, Enfield, EN1 1DW

All employees and volunteers are to be made fully aware of this policy and their duties and responsibilities under it. All employees and volunteers will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.