Age Concern Liverpool & Sefton
GDPR Data Protection Policy

Throughout this policy we may make reference to Age Concern Liverpool & Sefton, the Organisation or ACL&S. This means however that the policy is applicable to the Charity, Age Concern Liverpool & Sefton, the trading company, Age Concern Liverpool (Services) Ltd and any subsequent company within the group

---

1. Scope

Age Concern Liverpool & Sefton and its management and Board of Trustees, with a registered address at 58 Breckfield Road South, are committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well to safeguarding the "rights and freedoms" of persons whose information Age Concern Liverpool & Sefton collects pursuant to the General Data Protection Regulation ("GDPR") through the use of a Customer Record Management System ("CRMS"), which is developed, implemented, maintained and periodically reviewed and amended by Age Concern Liverpool & Sefton's Board of Directors.

The CRMS shall take into consideration the following: organisational structure, management responsibility, jurisdiction and geographical location and may comprise of a defined part of Age Concern Liverpool & Sefton or Age Concern Liverpool & Sefton as a whole.

2. Objectives

Age Concern Liverpool & Sefton's objectives for the CRMS are as follows:

1. To enable Age Concern Liverpool & Sefton to meet its personal data obligations in line with GDPR.

2. To support Age Concern Liverpool & Sefton's objectives;

3. To set appropriate systems and controls according to Age Concern Liverpool & Sefton's risk appetite;

4. To ensure that Age Concern Liverpool & Sefton is compliant with all applicable obligations, whether statutory, regulatory, contractual and/or professional; and

5. To safeguard personnel and stakeholder interests.

3. Good practice

Age Concern Liverpool & Sefton shall ensure compliance with data protection legislation and good practice, by at all times:

1. Processing personal information only when to do so is absolutely necessary for organisational purposes;

2. Ensuring that the least possible amount of personal data is collected, and that personal data is never processed unduly;

3. Informing individuals of how their personal data is or will be used and by whom;

4. Processing only pertinent and adequate personal data;

5. Processing personal data in a lawful and fair manner;

6. Keeping a record of the various categories of personal data processed;

7. Ensuring that all personal data that is kept is accurate and up-to-date;

8. Retaining personal data no longer than required by statute or regulatory body, or for organisational purposes;

9. Giving individuals the right of 'subject access', as well as all other individual rights pertaining to their personal data;

10. Ensuring that all personal data is maintained securely;

11. Transferring personal data outside of the EU only in situations where it shall be appropriately secured;

12. Applying various statutory exemptions, where appropriate;

13. Implementing a Customer Information Management System (CIMS), pursuant to this Policy;

14. Identifying stakeholders, both internal and external, and ascertaining their involvement within the operation of the CIMS; and

15. Identifying personnel that are responsible and accountable for the CIMS.

4. Notification

Age Concern Liverpool & Sefton has registered with the Information Commissioner as a data controller that engages in processing personal information of data subjects. Age Concern Liverpool & Sefton has identified all of the personal data that it processes and recorded it in its Data Inventory Schedule.

The Administration Manager shall retain a copy of all notifications made by Age Concern Liverpool & Sefton to the Information Commissioner's Office ("ICO").

The ICO notification shall be reviewed on an annual basis and the Chief Executive (CEO)/Chief Operating Officer (COO) shall be responsible for each annual review of the details of the notification, keeping in mind any changes to Age Concern Liverpool & Sefton's activities. These changes shall be ascertained by reviewing the Data Inventory Schedule and the management review. Data protection impact assessments shall be used to ascertain any additional relevant requirements.

This policy applies to all employees of Age Concern Liverpool & Sefton, including contractors and subcontractors. Breaches of the GDPR policy, including this CIMS policy, shall be dealt with according to Age Concern Liverpool & Sefton's Disciplinary Policy. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for Age Concern Liverpool & Sefton who have or may have access to personal data are required to read, understand and fully comply with this policy at all times. All aforementioned third parties are required to enter into a data confidentiality agreement prior to accessing any personal data. The data protection

obligations imposed by the confidentiality agreement shall be equally onerous as those to which Age Concern Liverpool & Sefton has agreed to comply with. Age Concern Liverpool & Sefton shall at all times have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

To assist all employees, trustees and volunteers with their responsibilities in this area, training in GDPR will be delivered. Employees and trustees will complete a full online training course. In the case of volunteers, it is acknowledged that they may not receive full online GDPR training. Consequently, volunteers will receive their GDPR training as part of their induction process, for which they will sign a document confirming that they have completed this.

5. GDPR background

The purpose of the GDPR is to ensure the "rights and freedoms" of living individuals, and to protect their personal data.

6. Definitions (as per the GDPR)

- *Data controller* may be a natural or legal person, whether a public authority, agency or other body which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data shall be processed. Where EU or Member State law predetermines the purposes and means of processing personal data, the data controller or, if appropriate, the specific criteria for selecting the data controller, may be provided for by EU or Member State law.

- *Data subject* refers to any living person who is the subject of personal data (see above for the definition of 'personal data') held by an 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.

- *Data subject consent* refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

- *Establishment* refers to the administrative head office of the 'data controller' in the EU, where the main decisions regarding the purpose of its data processing activities are made. 'Data controllers' based outside of the EU are required to

appoint a representative within the jurisdiction in which they operate to act on its behalf and liaise with the relevant regulatory and supervisory authorities.

- *Filing system* refers to any personal data set which is accessible on the basis of certain benchmarks, or norms and can be centralised, decentralised or dispersed across various locations.

- *Personal data* – means any information relating to a data subject.

- *Personal data breach* refers to a security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully. All personal data breaches must be reported to relevant regulatory authority by the 'data controller' at all times, whereas the data subject need only be informed of a data breach when it is likely that the breach will have an adverse effect on his or her privacy or personal data.

Breach Notification Procedure
This procedure applies in the following events:

1. A personal data breach pursuant to Article 33 '*Notification of a personal data breach to the supervisory authority',* and

2. A personal data breach pursuant to Article 34 *'Communication of a personal data breach to the data subject'* of the GDPR.

All users, including temporary employees of Age Concern Liverpool & Sefton and third parties, and Age Concern Liverpool & Sefton must be aware of this procedure and are required to follow it should a personal data breach incident occur.

All personal data breaches by Age Concern Liverpool & Sefton must be notified to the appropriate data controller immediately. The Chief Executive (CEO)/Chief Operating Officer (COO) must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

All personal data breaches by Age Concern Liverpool & Sefton must be notified to the appropriate supervisory authority immediately.

Age Concern Liverpool & Sefton is required to carry out an assessment in order to determine whether the personal data breach is likely cause a risk to the affected data subject's rights and freedoms under the GDPR. If a risk is considered likely, Age Concern Liverpool & Sefton is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after the risk assessment. If the notification is made outside of the 72 hour window, Age Concern Liverpool & Sefton is required to provide reasons for the delay.

Pursuant to the External Breach Notification Record, Age Concern Liverpool & Sefton is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Age Concern Liverpool & Sefton to address and/or mitigate the breach; and
- All other information regarding the data breach.

The CEO/COO must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether my email, telephone call etc.), to whom and how the confirmation of receipt was provided.

If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the GDPR, Age Concern Liverpool & Sefton is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;

- The name and contact details of the DPO;
- The likely outcomes of the personal data breach;
- Any measures taken by Age Concern Liverpool & Sefton to address and/or mitigate the breach; and
- All other information regarding the data breach.

Age Concern Liverpool & Sefton must use appropriate measures, such as encryption or password protection, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority.

Where possible pseudonymisation should be used. Pseudonymisation is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. For example, instead of using a name and address to identify a record, we may identify it as record number 1 and store the name and address details separately in a secure password protected and\or encrypted file which identifies that these personally identifiable details belong to record number 1. This can add a further layer of data security.

Age Concern Liverpool & Sefton must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

If notification would require Age Concern Liverpool & Sefton to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, so long as all data subject are effectively informed.

It is possible that the supervisory authority may require Age Concern Liverpool & Sefton to communicate the personal data breach to the data subject, should there be an element of high risk involved.

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

- *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 a 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.

- *Special categories of personal data* refers to personal data covering such matters as racial or ethnic origin, beliefs - whether religious, political or philosophical - membership of a trade-union and data relating to genetics, biometric identification, health, sexual orientation and sex life.

- *Territorial scope* the GDPR applies to all EU based 'data controllers' who engage in the processing of data subjects' personal data as well as to 'data controllers' located outside of the EU that process data subjects' personal data so as to provide goods and services, or to monitor EU based data subject behaviour.

- *Third party* is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.

7. Responsibilities under the GDPR

Age Concern Liverpool & Sefton is a data controller pursuant to the GDPR.

Appointed employees of Age Concern Liverpool & Sefton with managerial or supervisory responsibilities are responsible for ensuring that good personal data handling practices are developed, reviewed and encouraged within Age Concern Liverpool & Sefton, as per their individual job descriptions.

Data Controller

The position of Data Controller which involves the management of personal data within Age Concern Liverpool & Sefton as well as compliance with the requirements of the DPA and demonstration of good practice protocol, is to be taken up by the CEO/COO.

The Data Controller reports to Age Concern Liverpool & Sefton's Board of Directors and, amongst other things, is accountable for the development and implementation of the CIMS and for day-to-day compliance with this policy, both in terms of security and risk management. In addition, the Data Controller, is directly responsible for ensuring that Age Concern Liverpool & Sefton is GDPR compliant and that managers and executive officers

of Age Concern Liverpool & Sefton are compliant in respect of data processing that occurs within their field of responsibility and/or oversight.

The Data Controller shall at all times be the first point of contact for any employees of Age Concern Liverpool & Sefton who require guidance in relation to any aspect of data protection compliance.

The Data Controller is also responsible for other procedures, such as the Subject Access Request Policy.

It is not merely the Data Controller who is responsible for data protection, indeed all employees, volunteers and Directors of Age Concern Liverpool & Sefton who process personal data are responsible for ensuring compliance with data protection laws. Age Concern Liverpool & Sefton's GDPR Training Policy provides for specific training for employees, volunteers and Directors.

Risk Assessment

It is vital that Age Concern Liverpool & Sefton is aware of all risks associated with personal data processing and it is via its risk assessment process that Age Concern Liverpool & Sefton is able to assess the level of risk. Age Concern Liverpool & Sefton is also required to carry out assessments of the personal data processing undertaken by other organisations on its behalf and to manage any identified risks, so as to mitigate the likelihood of potential non-compliance with this policy.

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, Age Concern Liverpool & Sefton is required to engage in a risk assessment of the potential impact. More than one risk may be addressed in a single assessment (also known as a 'Data Protection Impact Assessment' ("DPIA")).

If the outcome of a DPIA points to a high risk that Age Concern Liverpool & Sefton's intended personal data processing could result in distress and/or may cause damage to data subjects, it is up to the Data Controller to decide whether Age Concern Liverpool & Sefton ought to proceed and the matter should be escalated to him or her. In turn, the Data Controller may escalate the matter to the regulatory authority if significant concerns have been identified.

It is the role of the Data Controller to ensure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an

acceptable level, as per the requirements of the GDPR and Age Concern Liverpool & Sefton's documented risk acceptance criteria.

Specific training

Age Concern Liverpool & Sefton is responsible for ensuring that all employees who are responsible, on a day-to-day basis, for compliance with the General Data Protection Regulation (GDPR) and relevant good practice, are able to exhibit competency in their understanding of the GDPR, good practice and the implementation thereof by Age Concern Liverpool & Sefton.

All persons with GDPR responsibility shall receive appropriate training and all training records are to be maintained by Age Concern Liverpool & Sefton's HR Department.

Age Concern Liverpool & Sefton shall also be responsible for ensuring that all persons with GDPR responsibility are regularly informed of and updated on all relevant matters related to personal data management, including through contact with external bodies, the most noteworthy of which is the Information Commissioner's Office (www.ico.gov.uk).

General training

Age Concern Liverpool & Sefton is responsible for ensuring that all of its employees are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with Age Concern Liverpool & Sefton's procedures.

To this end, Age Concern Liverpool & Sefton shall ensure that all of its employees are given appropriate and relevant training. It shall be the duty of Age Concern Liverpool & Sefton's HR Department to organise both specific training for GDPR responsible persons as well as general training for all staff and to maintain records of attendance.

8. Principles of data protection

The principles of personal data processing are as follows:

1. All personal data must be processed lawfully and fairly at all times, as per Age Concern Liverpool & Sefton's Fair Processing Policy.

2. Policies must also be transparent, meaning that Age Concern Liverpool & Sefton must ensure that its personal data processing policies, as well as any specific information provided to a data subject, are readily available, easily accessible and clear, drafted using clear and plain language.

3. The data subject must be provided with the following information:

    a. *Controller* - the identity and contact details of the Data Controller and any of its representatives;

    b. *Purpose* - the purpose or purposes and legal basis of processing;

    c. *Storage period* - the length of time for which the data shall be stored;

    d. *Rights* - confirmation of the existence of the following rights:
        i. Right to request access;
        ii. Right of rectification;
        iii. Right of erasure; and the
        iv. Right to raise an objection to the processing of the personal data;

e. *Categories* - the categories of personal data;

f. *Recipients* - the recipients and/or categories of recipients of personal data, if applicable;

g. *Location* - if the controller intends to make a transfer of personal data to a third country and the levels of data protection provided for by the laws of that country, if applicable; and

h. *Further information* - any further information required by the data subject in order to ensure that the processing is fair and lawful.

4. Personal data may only be collected for specified, explicit and legitimate reasons. When personal data is obtained for specific purposes, it must only be used in relation to that purpose and cannot be different from the reasons formally notified to the Information Commissioner, as part of Age Concern Liverpool & Sefton's GDPR ICO registration.

5. Personal data must be adequate, relevant and restricted to only what is required for processing. In relation to this, the Data Controller shall at all times:

a. Ensure that personal data which is superfluous and not necessarily required for the purpose(s) for which it is obtained, is not collected;

b. Approve all data collection forms, whether in hard-copy or electronic format;

c. Carry out an annual review of all methods of data collection, checking that they are still appropriate, relevant and not excessive; and

d. Securely delete or destroy any personal data that is collected in a manner that is excessive or unnecessary according to Age Concern Liverpool & Sefton's GDPR policies.

6. Personal data must be accurate and up-to-date:

a. Data should not be kept unless it is reasonable to assume its accuracy and data that is kept for long periods of time must be examined and amended, if necessary;

b. All staff must receive training from the Age Concern Liverpool & Sefton to ensure they fully understand the importance of collecting and maintaining accurate personal data;

c. Individuals are personally responsible for ensuring that the personal data held by Age Concern Liverpool & Sefton is accurate and up-to-date. Age Concern Liverpool & Sefton will assume that information submitted by individuals via data collection forms is accurate at the date of submission;

d. All employees of Age Concern Liverpool & Sefton are required to update the HR department as soon as reasonably possible of any changes to personal information, to ensure records are up-to-date at all times;

e. The Data Controller must ensure that relevant and suitable additional steps are taken to ensure that personal data is accurate and up-to-date;

f. The Data Controller shall, on an annual basis, carry out a review of all personal data controlled by Age Concern Liverpool & Sefton, referring to the Data Inventory Register and ascertain whether any data is no longer required to be held for the purpose notified to the ICO, arranging for that data to be deleted or destroyed in a safe manner.

g. The Data Controller shall also ensure that where inaccurate or out-of-date personal data has been passed on to third parties, that the third parties are duly informed and instructed not to use the incorrect or out-of-date information as a means for making decisions about the data subject involved. The Data Controller shall also provide an update to the third party, correcting any inaccuracies in the personal data.

7. The form in which the personal data is stored must be such that the data subject can only be identified when it is necessary to do so for processing purposes. The following principles apply:

   a. Personal data that is kept beyond the processing date must be either password protected and or encrypted or pseudonymised and kept to an absolute minimum, to ensure the protection of the data subject's identity should a data breach incident occur;

b. Personal data must be retained according to the Retention Requirements Policy and must be destroyed or deleted in a secure manner as soon as the retention date has passed; and

c. If a demonstrable need to retain records beyond the Records Retention limits arises, the only person authorised to agree this is the CEO/COO and reasons will be clearly aligned with GDPR principles.

8. The processing of personal data must always be carried out in a secure manner.

9. Personal data should not be processed in an unauthorised or unlawful manner, nor should it be accidentally lost or destroyed at any time and Age Concern Liverpool & Sefton shall implement robust technical and organisational measures to ensure the safeguarding of personal data.

9. Security controls

Security controls are necessary to ensure that risks to personal data identified by Age Concern Liverpool & Sefton are appropriately mitigated as much as possible to reduce the potential for damage or distress to data subjects whose personal data is being processed and are subject to regular audit and review. Please refer to Age Concern Liverpool & Sefton's Information Governance Policy.

Personal data shall not be transferred to a country outside of the EU unless the country provides appropriate protection of the data subject's 'rights and freedoms' in relation to the processing of personal data.

10. Adequacy of transfer

When using the Age Concern Liverpool & Sefton website, the information which you provide to us may be transferred to countries outside the European Union ("EU"). By way of example, this may happen if any of our servers are from time to time located in a country outside of the EU. If a situation arose whereby this transfer might be likely, to a country where GDPR or Privacy Shield are not applicable, we would always make contact with you, in advance, to seek your consent. If your consent was withheld, we would remove your details, prior to transfer.

Safeguards (Prior to determining if consent is required)

1. Assessing the adequacy of the transfer, by reference of the following:

- The nature of the personal data intended to be transferred;
- The country of origin and country of intended destination;
- The nature and duration of the personal data use;
- The legislative framework, codes of practice and international obligations of the data subject's country of residence; and
- (UK only) the security measures to be implemented in the country of intended destination in relation to the personal data.

2. Binding corporate rules

Age Concern Liverpool & Sefton is free to implement approved binding corporate rules in relation to personal data transfer outside of the EU, however only with prior permission from the relevant regulatory body.

3. Model contract clauses

Age Concern Liverpool & Sefton is free to implement model contract clauses in relation to personal data transfer outside of the EU and there will be an automatic recognition of adequacy of transfer, should the model contract clauses receive approval from the relevant regulatory body.

Exceptions

In the absence of an adequacy decision, including binding corporate rules and model contract clauses, no transfer of personal data to a non-EU country may take place unless one of the following preconditions is satisfied:

1. Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved in light of appropriate safeguards and an adequacy decision;

2. The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented;

3. The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;

4. The personal data transfer is in the public interest;

5. The personal data transfer is required for the creation, exercise or defence of legal claims;

6. The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons;

7. The personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled.

The following procedure must be followed to engage in the transfer of personal data to countries or to international organisations outside of the EU for processing, as per the requirements of the GDPR, including the transfer of personal data from a country or an international organisation to another country or another international organisation.

Age Concern Liverpool & Sefton, as data controller or data processor, shall ensure that adequate protection is provided to the data subject whose personal data is being transferred to countries or to international organisations outside of the EU by ensuring the following:

1. That it has checked the *Official Journal of the European Union* and confirmed that the country of the recipient of the personal data is an approved country, as per the EU list of approved countries. This also applies to industry sectors within particular countries;

2. That the country of the recipient of the personal data has adequate data protection systems and controls, whether by statute or self-regulation;

3. Through our contracting processes we have ensured that it is the responsibility of our IT company to ensure that when data is transferred outside of the EU that it is done in accordance with the requirements of the General Data Protection Regulations.

4. That it is transferring the personal data pursuant to approved binding corporate rules;

5. That it is applying one of the exemptions set out at clause 10 of the Age Concern Liverpool & Sefton GDPR Data Protection Policy, namely that:

    a. Explicit consent has been provided by a fully informed data subject, who has been made aware of all possible risks involved in light of appropriate safeguards and an adequacy decision;
    b. The personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject or when the data subject requests that pre-contractual measures are implemented;

    c. The personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;

    d. The personal data transfer is in the public interest;

    e. The personal data transfer is required for the creation, exercise or defence of legal claims;

    f. The data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions and the personal data transfer is necessary for the protection of the key interests of the data subject or of other persons, whether natural legal; and

    g. The personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest, but only so far as the legal requirements for consultation are fulfilled; and

6. That it is relying on approved certification mechanisms or codes of conduct alongside binding agreements in the country or international organisation outside of the EU that set out appropriate safeguards for the protection of the rights of personal data subjects.

11. Accountability

According to the GDPR accountability principle, the data controller is responsible both for ensuring overall compliance with the GDPR and for demonstrating that each of its processes is compliant with the GDPR requirements. To this extent data controllers are required to:

- Maintain all relevant documentation regarding its processes and operations;
- Implement proportionate security measures;
- Carry out Data Processing Impact Assessments (“DPIAs”);
- Comply with prior notification requirements;
- Seek the approval of relevant regulatory bodies; and
- Appoint a DPO where required.

12. The rights of data subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded:

1. The right to make access requests in respect of personal data that is held and disclosed;

2. The right to refuse personal data processing, when to do so is likely to result in damage or distress;

3. The right to refuse personal data processing, when it is for direct marketing purposes;

4. The right to be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;

5. The right not to solely be subject to any automated decision making process;

6. The right to claim damages should they suffer any loss as a result of a breach of the provisions of the GDPR;

7. The right to take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data;

8. The right to request that the ICO carry out an assessment as to whether any of the provisions of the GDPR have been breached;

9. The right to be provided with personal data in a format that is structured, commonly used and machine-readable;

10. The right to request that his or her personal data is sent to another data controller; and

11. The right to refuse automated profiling without prior approval.

13. Data access requests

Age Concern Liverpool & Sefton's Subject Access Request Policy sets out the procedure for making data access requests to data subjects and outlines how Age Concern Liverpool & Sefton will comply with the requirements of the GDPR regarding this.

14. Complaints

All complaints about the Age Concern Liverpool & Sefton's processing of personal data may be lodged by a data subject directly with the Data Controller, by filling in the appropriate form providing details of the complaint. The data subject must be provided with a Fair Processing Policy at this stage.

Complaints may also be made by a data subject directly to the relevant regulatory body and Age Concern Liverpool & Sefton will provide the relevant contact details dependent on the particular regulatory body for the function concerned.

All complaints in relation to how a complaint has been handled and any appeals following the submission of a complaint pertaining to information\data handling shall be dealt with by the Data Controller and the data subject is required to submit a further complaint.

15. Consent

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

- 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;
- Explicit;
- Specific;
- A clear and unambiguous indication of the wishes of the data subject;
- Informed;
- Provided either in a statement or by unambiguous affirmative action;
- Demonstrated by active communication between the data controller and the data subject and must never inferred or implied by omission or a lack of response to communication;
- In relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

Employees

Usually, Age Concern Liverpool & Sefton will obtain consent to process personal and sensitive data when a new employee signs an employment contract or during induction programmes. Data subjects have the right to withdraw consent at any time.

Other data subjects – Customers, service users and supporters

If using Consent as a condition to process data Age Concern Liverpool & Sefton will obtain Consent in accordance with the procedures outlined in the policy framework. Consent is considered to be a positive action on behalf of the data subject having read a clear, transparent and unambiguous privacy notice. It does not necessarily have to be a box that is ticked, it could be the completion of a form, or the supply of contact information. We understand that according to the Privacy and Electronic Communications Regulations (PECR), consent does not have to be explicit. We will use our judgement to decide how to obtain consent in different circumstances. However, we will always uphold the rights and freedoms of data subjects by always making it as easy to opt-out as it ever was to opt-in.

We mostly use Consent when promoting the aims and objectives of our organisation, Age Concern Liverpool & Sefton. We reserve the right to use it wherever we believe a data subject has indicated their wishes and where we have collected the data for that particular purpose. We only use data for the purpose for which it was collected.

Withdrawal of consent is indicated via the Data Subject Withdrawal of Consent Form and Age Concern Liverpool & Sefton must be able to demonstrate that the data subject has withdrawn consent, by producing the completed form, if required.

If Age Concern Liverpool & Sefton was processing the data for multiple purposes, Age Concern Liverpool & Sefton must be able to show that consent has been withdrawn for all purposes.

16. Data security

All employees of Age Concern Liverpool & Sefton are personally responsible for keeping secure any personal data held by Age Concern Liverpool & Sefton for which they are responsible. Under no circumstances may any personal data be disclosed to any third party unless Age Concern Liverpool & Sefton has provided express authorisation.

Accessing and storing personal data

Access to personal data shall only be granted to those who need it and only according to the principles of the Age Concern Liverpool & Sefton's Access Policy.

All personal data must be stored:

- In a locked room, the access to which is controlled; and/or
- In a locked cabinet, drawer or locker; and/or
- If in electronic format and stored on a computer, then either encrypted and/or password protected according to the corporate requirements set out in the Access Control Policy; and/or
- If in electronic format and stored on removable media, encrypted and/or password protected as per the Disposal of Removable Storage Media Procedure

Before being granted access to any organisational data, all staff of Age Concern Liverpool & Sefton must understand and have a copy of the Access Policy.

Computer screens and terminals must not be visible to anyone other than staff or volunteers of Age Concern Liverpool & Sefton with the requisite authorisation.

No manual records may be accessed by unauthorised employees of Age Concern Liverpool & Sefton and may not be removed from the business premises in the absence of explicit authorisation. Manual records must be removed from secured archiving when access is no longer needed on a day-to-day basis.

All deletion of personal data must be carried out in accordance with Age Concern Liverpool & Sefton's Retention Requirements. Manual records which have passed their retention date must be shredded and disposed of as 'confidential waste' and any removable or portable computer media such as hard drives as USB sticks must be wiped or destroyed as per the Disposal of Removable Storage Media Policy.

Personal data that is processed 'off-site' must be processed by authorised Age Concern Liverpool & Sefton staff, due to the increased risk of its loss, damage or theft.

17. Data access rights

Data subjects have the right to access all personal data in relation to them held by Age Concern Liverpool & Sefton, whether as manual records or electronic format. Data subjects therefore may at any time request to have sight of confidential personal references held by Age Concern Liverpool & Sefton as well as any personal data received by Age Concern Liverpool & Sefton from third-parties. To do so, a data subject must submit a Subject Access Request, as per the Subject Access Request Policy.

18. Disclosure of data

Age Concern Liverpool & Sefton must take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the Police. All employees of Age Concern Liverpool & Sefton are trained in order to learn how to exercise due caution when requested to disclose personal data to a third party.

Disclosure is permitted by the GDPR without the consent of the data subject under certain circumstances, namely:

- In the interests of safeguarding national security;
- In the interests of crime prevention and detection which includes the apprehension and prosecution of offenders;
- In the interests of assessing or collecting a tax duty;
- In the interests of discharging various regulatory functions, including health and safety;

- In the interests of preventing serious harm occurring to a third party; and
- In the interests of protecting the vital interests of the data subject i.e. only in a life and death situation.

The Data Controller is responsible for handling all requests for the provision of data for these reasons and authorisation by the Data Controller shall only be granted with support of appropriate documentation.

19. Data retention and disposal

Age Concern Liverpool & Sefton must not retain personal data for longer than is necessary and once an employee has left Age Concern Liverpool & Sefton, it may no longer be necessary for Age Concern Liverpool & Sefton to retain all of the personal data held in relation to that individual. Some data will be kept longer than others, in line with Age Concern Liverpool & Sefton's data retention and disposal procedure.

Disposal Procedure
This procedure covers all situations involving the disposal of removable storage media. Age Concern Liverpool & Sefton must ensure that all removable storage media are cleaned before being disposed of.

It is the responsibility of Age Concern Liverpool & Sefton's Administration Manager to manage the secure disposal of all storage media that is no longer required, according to this procedure. The Administration Manager is also the owner of the relationship with the approved third party contractor who removes shredded documents.

All owners of removable storage media are responsible for disposing of removable storage media according to this procedure.

1. Hard disks must be formatted and cleaned of all data and software before being reused or disposed of.

2. The secure disposal of disposable storage media as well as the disposal of all data processing equipment is the responsibility of the Administration Manager.

3. The Administration Manager will keep a log demonstrating what media has been destroyed or disposed of, when and by whom.

4. Hard disks are cleaned and guaranteed by an external third party, currently Britannia.

5. Removable storage media devices that contain confidential information must be subjected to a risk assessment before they are sent for repair in order to establish whether they ought to be repaired or replaced.

6. All media must be disposed of according to the legal and regulatory requirements for the disposal of computer equipment, via CDL (Computer Disposals Ltd.), Age Concern Liverpool & Sefton's approved disposal company.

7. Documents that contain confidential and restricted information should be deposited in the confidential waste by their owners prior to being destroyed. The confidential waste cupboard is locked and located in the main office. The confidential waste must be removed by an approved service provider, currently Bulky Bob's Office and Commercial Waste.

20. Document owner

The CEO/COO is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 7 February 2020 is available to all employees of Age Concern Liverpool & Sefton on the corporate intranet.

This policy document was approved by Age Concern Liverpool & Sefton's Policy Scrutiny Committee which is composed of Trustees, and is issued by the CEO/COO on a version controlled basis.

Review of this Policy

We keep this Policy under regular review. This Policy was last updated in February 2020.

Owner: CEO/COO
Reviewed: February 2020
Review Due: February 2021
Version: 4