Policy and Procedure 34
GDPR Data Retention

1. **Introduction**

This Policy sets out the obligations of Ayr Housing Aid Centre SCIO, a company registered in Scotland and a Scottish Charitable Incorporated Organisation under number SC049609, whose registered office is at 7 York Street, Ayr KA8 8AN ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company for specific purposes, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy and Procedure 31.

2. **Aims and Objectives**

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. **Scope**

3.1 This Policy applies to all personal data held by the Company OR [AND by third-party data processors processing personal data on the Company's behalf**.**

3.2 Personal data, as held by the Company **OR** the above is stored in the following ways and in the following locations:

a) The Company's servers, located on site

b) Computers permanently located in the Company's premises 7 York Street, Ayr

c) Laptop computers and other mobile devices provided by the Company to its employees;

d) Physical records stored locked filing cabinets;

4. **Data Subject Rights and Data Integrity**

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy and Procedure 31.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in Parts 12 and 13 of the Company's Data Protection Policy and Procedure 31, and how long the Company will hold that personal data or, if no fixed retention period can be determined this will be discussed with the data subject.

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of notwithstanding the retention periods otherwise set by this Data Retention Policy, the right to restrict the Company's use of their personal data, the right to data portability, and further rights as set out in Parts 14 to 20 of the Company's Data Protection Policy and Procedure 31.

5. **Technical and Organisational Data Security Measures**

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to Parts 20 to 22 of the Company's Data Protection Policy and Procedure 31 for further details:

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in

advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using recorded delivery or courier service.

h) All personal data transferred physically should be transferred in a suitable container marked "confidential";

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Senior Management (CEO or Services Manager),

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;

l) Personal data must be handled with care at all times and should not be left unattended or on view;

m) Computers used to view personal data must always be locked before being left unattended;

n) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of Senior Management (CEO or Services Manager) and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

o) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;

p) All personal data stored electronically should be backed up daily and weekly with backups stored onsite. All backups should be encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be changed regularly and must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

t) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

u) No software may be installed on any Company-owned computer or device without approval; and

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Part 21 of the Company's Data Protection Policy 31 for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely using the electronic shredding programme;

6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely using the electronic shredding programme;

6.3 Personal data stored in hardcopy form shall be shredded and securely disposed of;

6.4 Special category personal data stored in hardcopy form shall be shredded and securely disposed of.

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods and its retention periodically reviewed, as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Company's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

f) The potential risk to the data and impact of any loss.

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Sets	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
1 - 14	General Personal Data	Legitimate operations regarding Service users, Employees, Potential Employee, Former Employees, Management Committee and Volunteers	As per relevant Policies and Procedures	See Appendix 1 of Policy and Procedure 31 GDPR, different retention periods apply depending on circumstances	Retention and destruction are linked to the above Policy and Procedure
15 - 28	Personal Data held on Case Notes	To support the Service provided to Service Users and information necessary for the Service	Electronic - 3 years from case closure as per relevant Policies and Procedures	See Appendix 1 of Policy and Procedure 31 GDPR	Retention and destruction are linked to the above Policy and Procedure
29 - 46	Data held on Employees/Potential Employees, Management Committee and Volunteers	Legitimate Contractual obligations placed on the Centre	As per Policy and Procedure 32 Employees and general GDPR Policy and Procedure 31	See Appendix 1 of Policy and Procedure 31 GDPR. Employees/Volunteers up to 3 years after employment has ended. Management Committee 3 months after leaving. Potential Employees 3 months after Post has been filled. Complaints under Policy and Procedure 6 shall be retained for 2 years after complaint has been closed.	Retention and destruction are linked to the above Policy and Procedure

8. **Roles and Responsibilities**

8.1 The Company's Data Protection Officer's Telephone Number is 01292 288111.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be directly responsible for ensuring that relevant staff complies with the above data retention periods.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. **Implementation of Policy**

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

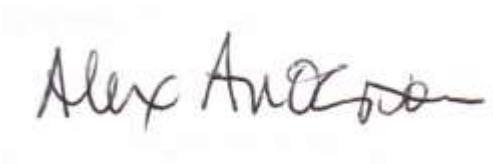
This Policy has been approved and authorised by:

Name: Alex Anderson

Position: Chairperson

Date: 16th May 2018

Due for Review by: 16th May 2020

Signature: 

Conversion to SCIO

Updated by CEO :- **9th October 2020**

Review date :- **10th October 2022**