

**Policy and Procedure 31
GDPR & Data Protection 2024**

1. Introduction

This Policy sets out the obligations of Ayr Housing Aid Centre SCIO (AHAC) regarding data protection and the rights of Service Users, Employees and Board (“data subjects”) in respect of their personal data under the General Data Protection Regulations (“the Regulation”) and the Data Protection Act 2018 (the DPA). This Policy will be updated when the Data Protection and Digital informal Bill has completed parliamentary process if changes are required. This Policy covers the UK as this is where we are based and store data. In the event any data is received and stored as per our P&P from people out with the UK we will comply with the relevant legislation and protections of that Country (e.g. EU, rest of the world). We will never transfer data out with the UK to any GDPR adequate countries or inadequate countries. The Centre is Cyber Essentials Accredited and Advice Pro is Information Security Code of Practice ISO27001 compliant. This should be read with Policy and Procedures 32, 33, 34.

The Regulation 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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by AHAC, its employees, agents, contractors, or other parties working on behalf of AHAC.

AHAC is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The 7 Data Protection Principles

This Policy aims to ensure compliance with the Regulation which sets out the following principles with which any party handling personal data must comply.

All personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (lawfulness, fairness, transparency)
- 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, in accordance with Article 89(1) not be considered to be incompatible with the initial purposes; (purpose limitation)
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; (data minimisation)
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay; (accuracy)
- 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 is 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject; (storage limitation)

- 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; (integrity & confidentiality)

3. Lawful, Fair, and Transparent Data Processing

3.1 The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract
- c) processing is necessary for compliance with a legal obligation to which the controller is subject
- d) processing is necessary to protect the vital interests of the data subject or of another natural person
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child or a vulnerable adult

3.2 If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, 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), at least one of the following conditions must be met:

The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless legislation prohibits);

- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with UK GDPR and Data Protection shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 AHAC collects and processes the personal data set out in this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject

communicates with us) and data received from third parties for example, South Ayrshire Council, DWP and Health Professionals. AHAC shall not communicate/share data with third parties without written consent freely given by data subject.

4.2 With regards to service users AHAC shall follow our Confidentiality Policy and Procedure 7. For this purpose Confidentiality Policy GDPR Form 1a or 1b (Prison Advice Service) shall be outlined to the data subjects and the different choices therein explain. Service user will be advised under what lawful processing heading we are processing their data set out in part 3 above. **The Services provided are not conditional on the signing of this form.**

4.3 AHAC only processes personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

4.4 AHAC has an accessible privacy notice and will advise data subjects of the lawful purpose/purposes we hold their personal data. Details of the Privacy Notice (Service User) can be accessed on our Data Protection tab at www.ayrhousingaidcentre.com. Alternatively data subjects can request written copies of the Privacy Notice (Service User). AHAC has a Privacy Notice (Staff, Former Staff and Applicants).

5. **Adequate, Relevant and Limited Data Processing**

AHAC will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. **Accuracy of Data and Keeping Data Up To Date**

AHAC and staff shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter by Senior Staff during case reviews. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. **Timely Processing**

AHAC shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed and will apply part 2(e) above. When the data is no longer required, all reasonable steps will be taken to erase it without delay. The Centre shall apply Policy and Procedure 34 (Retention and Destruction).

8. **Secure Processing**

AHAC shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy. The Centre shall apply Policy and Procedure 33 (IT Security). The Centre is Cyber Essentials Accredited and Advice Pro is Information Security Code of Practice ISO27001 compliant.

9. **Accountability**

9.1 AHAC Data Protection Officer can be contacted on 01292 288111.

9.2 AHAC shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- a) The name and details of AHAC, its Data Protection Officer, and any applicable third-party data controllers
- b) The purposes for which AHAC processes personal data
- c) Details of the categories of personal data collected, held, and processed by AHAC; and the categories of data subject to which that personal data relates
- d) Details of any third parties that will receive personal data from AHAC

- e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards
- f) Details of how long personal data will be retained by AHAC and
- g) Detailed descriptions of all technical and organisational measures taken by AHAC to ensure the security of personal data

The Index of Personal Data held by AHAC is attached as appendix 1 to this Policy and Procedure.

10. Privacy Impact Assessments

AHAC shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by AHAC's Data Protection Officer and shall address the following areas of importance:

- 10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data
- 10.2 Details of the legitimate interests being pursued by AHAC
- 10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
- 10.4 An assessment of the risks posed to individual data subjects and
- 10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

- a) right to be informed
- b) right of access
- c) right to rectification
- d) right to erasure (also known as the 'right to be forgotten')
- e) right to restrict processing
- f) right to data portability
- g) right to object
- h) rights with respect to automated decision-making and profiling

12. Keeping Data Subjects Informed

12.1 AHAC shall ensure that the following information is provided to every data subject when personal data is collected:

- a) Details of AHAC including, but not limited to, the identity of its Data Protection Officer
- b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in this Policy) and the legal basis justifying that collection and processing
- c) Where applicable, the legitimate interests upon which AHAC is justifying its collection and processing of the personal data
- d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed
- e) Where the personal data is to be transferred to one or more third parties, details of those parties
- f) Details of the length of time the personal data will be held by AHAC (or, where there is no predetermined period, details of how that length of time will be determined)
- g) Details of the data subject's rights under the Regulation

- h) Details of the data subject's right to withdraw their consent to AHAC's processing of their personal data at any time
- i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation)
- j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection

12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

- a) If the personal data is used to communicate with the data subject, at the time of the first communication or
- b) If the personal data is to be disclosed to another party, before the personal data is disclosed or
- c) In any event, not more than one month after the time at which AHAC obtains the personal data.

13. Data Subject Access

A data subject may make a subject access request ("SAR") at any time to find out more about the information which AHAC holds about them.

- SARs should be made in writing, addressed to Data Protection Officer, 7 York Street, Ayr KA8 8AN or telephone 01292 288111
- A SAR may be made using AHAC's Subject Access Request Form, but does not have to be, and if it is not, it should be clearly identifiable as a SAR
- SARs must make it clear whether it is the data subject themselves that is making the request or whether it is a person acting on his or her behalf. In either case, proof of identity must be provided. If the SAR is made on another's behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject

Upon receipt of a SAR AHAC shall have a maximum period of 1 month in which to respond fully but shall always aim to acknowledge receipt of SARs within 3 working days.

The following information will be provided to the data subject:

- Whether or not AHAC holds any personal data on the data subject
- A description of any personal data held on the data subject
- Details of what that personal data is used for
- Details of how to access that personal data and how to keep it up to date
- Details of any third-party organisations that personal data is passed to and
- Details of any technical terminology or codes

AHAC does not charge a fee for the handling of normal SARs. AHAC reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 If a data subject informs AHAC that personal data held by AHAC is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be

extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. Erasure of Personal Data

15.1 Data subjects may request that AHAC erases the personal data it holds about them in the following circumstances:

- a) It is no longer necessary for AHAC to hold that personal data with respect to the purpose for which it was originally collected or processed
- b) The data subject wishes to withdraw their consent to AHAC holding and processing their personal data
- c) The data subject objects to AHAC holding and processing their personal data (and there is no overriding legitimate interest to allow AHAC to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object)
- d) The personal data has been processed unlawfully
- e) The personal data needs to be erased in order for AHAC to comply with a particular legal obligation
- f) The personal data is being held and processed for the purpose of providing information social services to a child.

15.2 Unless AHAC has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that AHAC ceases processing the personal data it holds about them. If a data subject makes such a request, AHAC shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 AHAC processes personal data using word, excel, PDF and online formats (e.g. Advice pro, Breathe HR and Cloud secure systems and is securely held)

17.2 Where data subjects have given their consent to AHAC to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between AHAC and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.3 To facilitate the right of data portability, AHAC shall make available all applicable personal data to data subjects in the best format depending on the data, e.g. Word, Excel, PDF.

17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller by appropriate secure means.

17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to 2 months in the case of complex requests in the

case of complex or numerous requests and in such cases the data subject shall be informed of the need for the extension).

18. **Objections to Personal Data Processing**

- 18.1 Data subjects have the right to object to AHAC processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.
- 18.2 Where a data subject objects to AHAC processing their personal data based on its legitimate interests, AHAC shall cease such processing forthwith, unless it can be demonstrated that AHAC's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
- 18.3 Where a data subject objects to AHAC processing their personal data for direct marketing purposes, AHAC shall cease such processing forthwith.
- 18.4 Where a data subject objects to AHAC processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. AHAC is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. **Personal Data**

The following personal data may be collected, held, and processed by AHAC:

- a) Application, Shortlisting and Recruitment, This will facilitate the employment of staff within AHAC, data collected for this purpose will be erased within 3 months of the Post being filled. The Centre shall apply Policy and Procedure 34 (Retention and Destruction).
- b) Employees shall expressly consent to the collection of relevant data. All relevant data for employees shall be securely retained during employment, in addition relevant data will be shared with South Ayrshire Council in terms of services they provide for AHAC. In addition AHAC shall share relevant information with Strathclyde Pension Scheme or other pension providers. AHAC shall comply with all statutory PVG disclosure requirements.
- c) The Board shall comply with the requirements of Office of the Scottish Charities Regulator (OSCR) and maintain a list of Board members including addresses and contact numbers for the purpose of ensuring effective governance and control of AHAC.
- d) Service User, we shall collect relevant personal data of services users and apply part 4 of this Policy. The data collected is limited to the specific requirements and circumstances of the service user. The Centre will store the electronic Visitors Log for a period of 6 months.
- e) Statistical data drawn from personal data will be used for research, quality assurance and reporting purposes, this data is anonymised.

20. **Technical Data Protection Measures**

AHAC shall ensure that all of its employees, agents, contractors or other parties working on behalf of AHAC comply with the following when working with personal data:

- All emails containing sensitive data must be encrypted using word and/or excel;
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- 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 should be deleted. All temporary files associated therewith should also be deleted
- 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
- No personal data may be shared informally and if an employee, agent, sub-contractor or other party working on behalf of AHAC requires access to any personal data that they do not already

have access to, such access should be formally requested from Senior Management (CEO or Operations Manager)

- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar
- No personal data may be transferred to any employees, agents, contractors or other parties, whether such parties are working on behalf of AHAC or not, without the authorisation of CEO Operations Manager or Office & Finance Manager.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; IT Policy and Procedure 33 shall apply
- Any unwanted copies of personal data (i.e. printouts or electronic duplicates) that are no longer needed should be disposed of securely. Hardcopies should be shredded and electronic copies should be deleted using secure electronic shredding
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to AHAC or otherwise without the formal written approval of the Operations Manager and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary
- 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 AHAC where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Act which may include demonstrating to AHAC that all suitable technical and organisational measures have been taken
- All electronic copies of personal data should be stored securely using passwords and limited access through permissions
- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers and where possible symbols. All software used by AHAC is designed to require such passwords
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of AHAC, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff can assist in the reset process

All personal data held by AHAC shall be regularly reviewed for accuracy and completeness. Where AHAC has regular contact with data subjects, any personal data held about those data subjects should be confirmed as is necessary. If any personal data is found to be out of date or otherwise inaccurate, it should be updated and/or corrected immediately where possible. If any personal data is no longer required by AHAC, it should be securely deleted and disposed of by using electronic shredding programme and hard copies will be securely shredded to comply with Cyber Essentials Accredited and Advice Pro (Information Security Code of Practice ISO27001) AHAC shall apply Policy and Procedure 33 (IT Security).

21. Organisational Measures

AHAC shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data. AHAC has appointed a Data Protection Officer with the specific responsibility of overseeing data protection and ensuring compliance with this Policy and with the Act.

The Data Protection Officer shall in particular be responsible for:

- Overseeing the implementation of, and compliance with this Policy, working in conjunction with the relevant employees, managers and/or department heads, agents, contractors and other

parties working on behalf of AHAC

- Organising suitable and regular data protection training and awareness programmes within AHAC
- Reviewing this Policy and all related procedures not less than bi-annually
- All employees, agents, contractors, or other parties working on behalf of AHAC are made fully aware of both their individual responsibilities and AHAC's responsibilities under the Regulations and under this Policy, and shall be provided with a copy of this Policy
- Only employees, agents, sub-contractors, or other parties working on behalf of AHAC that need access to and use of personal data in order to carry out their assigned duties correctly shall have access to personal data held by AHAC
- All employees, agents, contractors, or other parties working on behalf of AHAC handling personal data will be appropriately trained to do so
- All employees, agents, contractors, or other parties working on behalf of AHAC handling personal data will be appropriately supervised
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed
- The Performance of those employees, agents, contractors, or other parties working on behalf of AHAC handling personal data shall be regularly evaluated and reviewed
- All employees, agents, contractors, or other parties working on behalf of AHAC handling personal data will be bound to do so in accordance with the principles of the regulations and this Policy by contract
- All agents, contractors, or other parties working on behalf of AHAC handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of AHAC arising out of this Policy and the Regulations
- Where any agent, contractor or other party working on behalf of AHAC handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless AHAC against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

22. **Data Breach Notification**

22.1 All personal data breaches must be reported immediately to AHAC's Data Protection Officer.

22.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

22.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 22.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

22.4 Data breach notifications shall include the following information:


- a) The categories and approximate number of data subjects concerned;
- b) The categories and approximate number of personal data records concerned;
- c) The name and contact details of AHAC's Data Protection Officer (or other contact point where more information can be obtained);
- d) The likely consequences of the breach;
- e) Details of the measures taken, or proposed to be taken, by AHAC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

23. Implementation of Policy

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

This Policy has been approved & authorised by:

Name: Alex Anderson **Position:** Chairperson **Date:** 16.5.18 **Review date:**16.5.20



Signature:

Conversion to SCIO

Updated by CEO -	9.10.20	Review date -	10.10.22
Reviewed by Senior Management -	12.8.21	Review date -	12.8.23
Reviewed by IT & HR Consultants -	18.1.24	Discussed at Board meeting	27.2.24
Reviewed by CEO & Chairperson -	22.5.24	Board approved –	28.5.24 Review date - 28.5.26

AYR HOUSING AID CENTRE SCIO

Appendix 1

IN DEPTH REVIEW OF PERSONAL DATA HELD BY THE CENTRE (Policy and Procedure 31)

GENERAL DATA PROTECTION & DATA PROTECTION LEGISLATION & REGULATIONS

No.	Data Set 1: General Personal Data ①	Service User An individual accessing Centre Services	Service User Household A member of a household accessing Centre Services	Employee An person employed with Centre Contract of Employment	Potential Employee ② An individual applying to become employed by the centre under Contract of Employment	Former Employee's ③ An individual who has left the Centre's employment	Volunteer An individual who has volunteered at the Centre	Board Trustees An individual who is serving on the Board of Trustees	Location Held in secure Electronic folder	Loss/Risk Introduce wide security measures, see IT Security Policy 33	Impact of Loss/SU Potential risk of personal data accessed from unauthorised third parties i.e. hackers	Impact of Loss/Centre Full security review, duty to inform Data Subjects of loss & take appropriate action. Initiate data recovery systems from back-ups	Retention See P&P on retention periods -	File Destruction Electronic Shredding Programme/Paper Shred in place carried out my Management
1	Name	X	X	X	X	X	X	X	Secure	1	Mitigated through Cyber Essentials and IT security	Mitigated through Cyber Essentials and IT security	Robust systems in place for data retention and secure electronic shredding processes	As above
2	Address	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
3	Contact Telephone Number	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
4	Email Address	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
5	D.O.B.	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
6	N.I. Number	X	X - only if required	X		X	X - only if required	X	As above	1	As above	As above	As above	As above
7	Gender	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
8	Internet Access	X							As above	1	As above	As above	As above	As above
9	Bank Account Access ④	X		X		X			As above	1	As above	As above	As above	As above
10	Disability/Health ⑤	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
11	Nationality	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
12	Ethnic Origin	X	X	X	X	X	X	X	As above	1	As above	As above	As above	As above
13	Domestic Abuse	X	X - only if required	X - only if required	X - only if required	X - only if required	X - only if required		As above	1	As above	As above	As above	As above
14	Employment Status	X	X - only if required	X	X	X		X	As above	1	As above	As above	As above	As above

① Data Set 1 data will only be gathered if it is necessary

② Potential Employees data erased 3 months following appointment of Post

③ Former Employees data within secure electronic system, electronic shred process in place

④ SU data only held if necessary for the purposes of paying grants, poverty alleviation etc - Board access to Bank accounts terminated on exit from Board

⑤ Any data on this is held securely and process for secure destruction on closure/exit

Key for Loss/Risk:

Low - 1 to 2

Medium - 3 to 4

High - 4 to 5

Reviewed 24.5.24 by SS & EG

		Service User	Service User Household	Employee	Potential Employee	Former Employee's	Volunteer	Board Trustees	Location	Loss/Risk	Impact of Loss/SU	Impact of Loss/Centre	Retention	File Destruction
No.	Data Set 2: Personal Data held on Case Notes ❶	An individual accessing Centre Services	A member of a household accessing Centre Services	An person employed with Centre Contract of Employment	An individual applying to become employed by the centre under Contract of Employment	An individual who has left the Centre's employment	An individual who has volunteered at the Centre	An individual who is serving on the Board of Trustees	Electronic	Introduce wide security measures, see IT Security Policy 33	Potential accessing of personal data from unathroised third parties i.e. hackers	Full security review, duty to inform Data Subjects of loss taking appropriate action. Initiate data recovery systems from back-ups	Electronic - SU's 3 Years from Case Closure via Advice Pro and internal systems	Secure Electronic Shredding Programme
15	Case Number	X	X - only if required						As above	1	As above	As above	As above	As above
16	Name	X	X - only if required						As above	1	As above	As above	As above	As above
17	Address	X	X - only if required						As above	1	As above	As above	As above	As above
18	Contact Telephone Number	X	X - only if required						As above	1	As above	As above	As above	As above
19	Email	X	X - only if required						As above	1	As above	As above	As above	As above
20	N.I Number	X	X - only if required						As above	1	As above	As above	As above	As above
21	Disability/Health	X - only if required	X - only if required						As above	1	As above	As above	As above	As above
22	Nationality	X	X - only if required						As above	1	As above	As above	As above	As above
23	Ethnic Origin	X	X - only if required						As above	1	As above	As above	As above	As above
24	Domestic Abuse	X	X - only if required						As above	1	As above	As above	As above	As above
25	Benefit Information/Source of Income	X - only if required	X - only if required						As above	2	As above	As above	As above	As above
26	Tenancy Agreement Information	X - only if required	X - only if required						As above	1	As above	As above	As above	As above
27	Other relevant details	X	X - only if required						As above	1	As above	As above	As above	As above
28	Service User's Documents ❷	X	X - only if required						As above	1	As above	As above	As above	As above
❶	Data Set 2 data will only be gathered if it is necessary and only relates to Service Users All documents are scanned and originals returned as per National Standards/Care Inspectorate and own P&P on data retention and safe, secure storage									Key for Loss/Risk:				
❷										Low - 1 to 2				
										Medium - 3 to 4				
										High - 4 to 5				
	Reviewed 24.5.24 by SS & EG													

No.	Data Set 3: Personal Data held on Employees/Volunteers ①	Service User An individual accessing Centre Services	Service User Household A member of a household accessing Centre Services	Employee An person employed with Centre Contract of Employment	Potential Employee ② An individual applying to become employed by the centre under Contract of Employment	Former Employee's ③ An individual who has left the Centre's employment	Volunteer An individual who has volunteered at the Centre	Board Trustees An individual who is serving on the Board of Trustees	Location Held in secure Electronic folder	Loss/Risk Introduce wide security measures, see IT Security Policy 33	Impact of Loss/SU Potential risk of personal data accessed from unauthorised third parties i.e. hackers	Impact of Loss/Centre Full security review, duty to inform Data Subjects of loss & take appropriate action. Initiate data recovery systems from back-ups	Retention See P&P on retention periods -	File Destruction Electronic Shredding Programme/Paper Shred in place carried out my Management
29	Name			X	X	X	X	X	As above	1	As above	As above	As above	As above
30	Address			X	X	X	X	X	As above	1	As above	As above	As above	As above
31	Contact Telephone Number			X	X	X	X	X	As above	1	As above	As above	As above	As above
32	Email			X	X	X	X	X	As above	1	As above	As above	As above	As above
33	D.O.B.			X	X	X	X	X	As above	1	As above	As above	As above	As above
34	N.I. Number			X	X	X	X	X	As above	1	As above	As above	As above	As above
35	Disclosures/PVG			X		X	X		As above	1	As above	As above	As above	As above
36	Car MOT and Insurance details			If applicable	If applicable	If applicable	If applicable		As above	1	As above	As above	As above	As above
37	Bank Account Details			X		X			As above	2	As above	As above	As above	As above
38	Supervision and Annual Appraisal Forms			X		Will be erased 3 months after end of employment			As above	1	As above	As above	As above	As above
39	Maternity/Paternity Forms			X		As above	If applicable		As above	1	As above	As above	As above	As above
40	Pension Opt Out Form			If applicable		If applicable			As above	1	As above	As above	As above	As above
41	P45			If applicable		If applicable			As above	1	As above	As above	As above	As above
42	Statement of Fitness for Work			If applicable		If applicable			As above	1	As above	As above	As above	As above
43	References			If applicable		If applicable			As above	1	As above	As above	As above	As above
44	Disciplinary			If applicable		If applicable	If applicable		As above	1	As above	As above	As above	As above
45	Grievance			X		If applicable	If applicable		As above	1	As above	As above	As above	As above
46	Complaints	X		X	X	X	X	X	As above	1	As above	As above	2 years	As above
①	Data Set 3 data will only be gathered if it is necessary													
②	Potential Employees data erased 3 months following appointment of Post													
③	Former Employees data within secure electronic system, electronic shred process in place													
	Reviewed 24.5.24 by SS & EG													
										Key for Loss/Risk:				
										Low - 1 to 2				
										Medium - 3 to 4				
										High - 4 to 5				