Policy and Procedure 7
Confidentiality Policy

This Policy should be read with our Data Protection GDPR Policy and Procedure No.31 and the Centre's commitment to privacy of service users. This information can be accessed on the Data Protection tab on our website www.ayrhousingaidcentre.com or on request, please contact the Centre on 01292 288111.

The Centre is committed to respecting the confidentiality of verbal or written information given by service users. In opening cases the Centre shall explain this Policy and exceptions to the Policy.

If initial contact is over the phone staff shall advise the service user of our confidentiality policy and exceptions to the Policy. The member of staff shall sign Confidentiality Form 1 after advising on the above and if further actions beyond the initial contact are required this Form should be sent to the service user with a stamped addressed envelope, e-mailed or other electronic means. Alternatively the service user should be requested to come into the Centre to sign form. This policy conforms to the Centre's Data Protection General Regulation Policy and Procedure number 31.

Terms of Policy

1. General

i. Information held by the Centre for casework is strictly confidential between the Centre and the user of the service. No information for any purposes will be shared with other organisations or authorities without the expressed and written consent of the user of the service. The service user shall complete Confidentiality GDPR Form 1a or 1b (Prison Advice Service). A user of the service can nominate a contact person concerning his case who will be able to receive relevant information; this should be in writing.

ii. Users of the service have the right to view anything recorded (written or saved on to a computer) by making a subject access request (SAR). For further information contact the Data Protection Officer. This in most cases will be provided within 1 month of the request. The Centre will not release third party information to a service user unless the third party gives permission.

iii. Staff will ensure that a Data Protection Form (Confidentiality GDPR Form 1a or 1b (Prison Advice Service) is completed and a summary of the GDPR Data Protection principles are offered to the service user.

2. Data Sharing

The Centre shall only share data with third parties if the data subject has explicitly consented. In the cases of one off requests the Centre will consider whether the sharing is justified and they will record contact with the service user and the decision on sharing. Exceptions to this rule apply as outlined in Part 4 of this Policy.

i. As part of monitoring and quality assurance a selection of case-files are audited by external auditors under the National Standards for Information and Advice. The user of the service must be advised of this process and asked to make a choice on whether they wish their file to be part of this process as per Confidentiality GDPR Form 1a or 1b (Prison Advice Service).

ii. Some Services within the Centre are registered with the Care Inspectorate and therefore subjected to unannounced Inspections. Inspectors can legally request access to relevant case files; in cases such as these Service Users will be advised of this potentially occurring. Service User's will be given the opportunity to state whether they approve.

iii. The Centre will ask whether a service user wishes their data to be shared with appropriate Local Authority systems to allow more efficient support to be provided to the service user. The service user will be asked to make a choice on whether they wish their file to be part of this process as per confidentiality GDPR Forms 1a or 1b (Prison Advice Service).

iv. If a user of the service or a member of staff considers that there has been a breach of confidentiality, this matter should be raised initially with the CEO or the Service Manager who will investigate the matter and report to the Management Committee. In the event that the breach concerns personal data as defined by GDPR this should be reported to the Data Protection Officer.

The service user will be kept informed of any developments concerning the case.

3. Data Breach Notification

All personal data breaches must be reported immediately to the Data Protection Officer. 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), 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.

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 22.2/22.3 of the Data Protection GDPR Policy and Procedure 31) to the rights and freedoms of data subjects, Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

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 the Company'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 the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

4. Exceptions

i. The Centre shall pass information to the relevant authorities if there are issues concerning the safety of a child (see Policy and Procedure 18) or a vulnerable adult (see Policy and Procedure 19). This includes allegations or charges brought against service user in relation to children or vulnerable adults. The procedure for reporting is as follows;

- Worker shall report concerns to Services Manager/Senior within 2 working days after becoming aware of potential safety issues concerning a child or vulnerable adult.

- If a member of staff considers there is imminent danger for a child they will contact Child Protection Officer at Social Work or the Police immediately applying Policy and Procedure 18.
- If a member of staff considers there is imminent danger to a vulnerable adult they will contact Social Work or the Police immediately applying Policy and Procedure 19.
- The Services Manager/Senior shall record incident in the incident log.
- The Services Manager/Senior shall consider appropriate action which will be recorded on incident log.
- If there is current social work involvement the appropriate allocated Social Worker should be contacted after discussion with CEO or the Services Manager. In any other case the CEO or the Services Manager will decide whether to refer to duty social work.
- In such circumstances the Centre shall apply its Data Protection GDPR Policy and Procedure No.31, Section 3f.

ii. If it is in the interests of the service user the member of staff shall discuss referral in part for additional support or the whole case, Policy and Procedure 9, Referrals shall apply.

Forms to be used are:-

1. Confidentiality Policy Form 1a
2. Confidentiality Policy Form 1b (Prison Advice Service)

Date of Policy: - **20th May 2003**
Approved by Committee: - **5th June 2003**
Amended by Committee:- **10th March 2005**
Amended by Committee: - **20th December 2005**
Amended by Committee: - **7th February 2008**
Amended by Committee: - **5th June 2008**
Amended by Committee: - **27th November 2008**
Amended by Committee: - **10th October 2013**
Reviewed by CEO: - **5th December 2015**
Review date:- **5th December 2017**
Reviewed by Advice Team: - **18th December 2017**
Reviewed by CEO/Office and Finance Manager: - **6th April 2018**
Reviewed by CEO/Office and Finance Manager: - **18th April 2018**
Approved by Committee: - **30th April 2018**
Review Date: - **30th April 2020**
Conversion to SCIO
Updated by CEO :- **9th October 2020**
Review date :- **10th August 2021**
Updated by CEO :- **12th October 2021**
Review date :- **12th October 2024**