The Anthony Seddon Fund
Supporting mental wellbeing in our community

Document Control	
Title:	**Access to Records Policy**
Version:	**3**
Reference Number:	**IG-004**

Scope:

This policy applies to all staff and volunteers who come into contact with customers or are in some way responsible for keeping or handling records.
This policy applies to all records, both manual and computerised.

Purpose:

The purpose of this policy is to provide processes to be followed by **The Anthony Seddon Fund** staff and volunteers when dealing with requests for access to records and to inform customers how to make a request for records.

Supersedes:

IG-004 – Access to Records Policy – V2

Version Changes:

- **Complete Review**: The policy has been thoroughly reviewed and updated to enhance clarity, structure, and comprehensiveness.
- **Purpose**: Clarified the purpose of the policy, emphasising the importance of compliance with GDPR and other relevant data protection laws.
- **Responsibilities, Accountabilities, and Duties**: Expanded to include the roles of the Data Protection Officer (DPO) and the Caldicott Guardian, providing clear definitions of responsibilities.
- **Request for Information from Solicitors**: Added specific procedures for handling requests from solicitors, including verification and confidentiality requirements.
- **Sending the Record to the Applicant**: Introduced subsections for postal, email, and in-person delivery methods, ensuring secure and verified handling.
- **Data Subject Rights**: A comprehensive overview of data subject rights under GDPR, including rights to access, rectification, erasure, and data portability.

Next Review Date:	June 2025

Contents

1. Introduction

Individuals have a right to apply for records that hold information about themselves. The Anthony Seddon Fund is committed to ensuring that adequate procedures are in place to enable customers to exercise this right in compliance with the General Data Protection Regulation (GDPR) and other relevant data protection laws.

The GDPR and Data Protection Laws provide living individuals with the right to access their own records. This right can also be exercised by an authorised representative on the individual's behalf. In most cases, the applicant will receive the information free of charge and within one calendar month of submitting the request. This policy outlines the processes to be followed by The Anthony Seddon Fund staff and volunteers when dealing with requests for access to records and informs customers on how to make a request for their records.

2. Purpose

The purpose of this policy is to provide clear procedures to be followed by The Anthony Seddon Fund staff and volunteers when dealing with requests for access to records. It also aims to inform customers about how they can make a request for their records in compliance with the GDPR and other relevant data protection laws.

It is crucial that all trustees, staff, and volunteers understand the requirements of the law and their roles in ensuring The Anthony Seddon Fund complies with these legal obligations. Compliance with this policy is a condition of employment, and any breach may result in disciplinary action.

Where the term 'record' is used, it refers to both manual files and electronic customer records. This policy ensures that all records, regardless of their format, are handled in accordance with GDPR, Data Protection Laws, and The Anthony Seddon Fund's commitment to transparency and accountability.

3. Responsibilities, Accountabilities and Duties

Trustee Board

The Trustee Board of The Anthony Seddon Fund has overall responsibility for the management of all records. They ensure that the organisation complies with the GDPR and other relevant data protection laws.

General Manager

The General Manager oversees the day-to-day management of this policy. This includes ensuring that requests for access to records are processed in accordance with legal requirements and organisational procedures.

Data Protection Officer (DPO)
The DPO is responsible for monitoring compliance with the GDPR and other data protection laws, as well as The Anthony Seddon Fund's data protection policies. The DPO also oversees the training and guidance for staff and volunteers on data protection issues.

Caldicott Guardian
The Caldicott Guardian ensures that personal information is used ethically and legally within the organisation. They are responsible for reviewing the use and sharing of personal information to ensure it aligns with the Caldicott Principles.

Staff and Volunteers
All staff and volunteers are responsible for adhering to this policy and ensuring that they handle records in compliance with GDPR and other data protection laws. This includes understanding and following the procedures for processing access requests and maintaining the confidentiality and security of records.

4. Receiving an Access Request Under GDPR

Subject Access Request (SAR)

Individuals have a right under the GDPR and Data Protection Laws to access certain personal data being kept about them on computers and in certain files. This is known as a Subject Access Request (SAR). Any person wishing to exercise this right should apply in writing to:
General Manager,
The Anthony Seddon Fund,
12 George Street,
Ashton-under-Lyne,
OL6 6AQ
The following information may be required before access is granted:

- Reason for the request (optional).
- Specific information required.
- Timescale.

Customers do not need to provide a reason for accessing their records but must provide sufficient information to enable the records to be located.

Proof of Identity
To protect the individual's privacy, proof of identity may be required before access is granted. Acceptable forms of ID include:

- Passport
- Driving License
- Birth Certificate

Processing the Request
The Anthony Seddon Fund aims to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 30 days required by the GDPR from receiving the written request.

Repeat Requests
Where an access request has previously been met, GDPR permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between them.

Who Can Make a Request for Records

Formal access to a record can be obtained by any of the following:

- The customer.
- A person having parental responsibility for a child (under 16), if the child is too young to make their own request, or it may be possible to accept such a request from the child themselves if they are judged competent (see **Section 5**).
- A person appointed by the court to manage the affairs of a customer who is incapable of managing their own affairs.
- An agent or representative (e.g., a solicitor or carer) acting on behalf of a capable customer with written authority to make the request on their behalf, or a person granted power of attorney by the customer.
- The customer's personal representative if the customer has died, and any other person who may have a claim arising out of the customer's death (see **Section 6**).

Other entities that may request access include:

- Criminal Injuries Compensation Authority (CICA) or Department for Work and Pensions (DWP).
- The police, under the Crime and Disorder Act (see **Section 7**).
- The Crown Prosecution Service (CPS).
- The court via an order.
- Other authorities or individuals authorised by the Caldicott Guardian.

Fees to Access Health Records

The GDPR states that The Anthony Seddon Fund must supply a copy of the information requested free of charge. However, a reasonable fee can be charged when the request is manifestly unfounded or excessive, particularly if it is repetitive. The Anthony Seddon Fund may also charge a reasonable fee to comply with requests for further copies of the same information.

Any fees charged must be based on the administrative cost of providing the information. If The Anthony Seddon Fund refuses to respond to a request, an explanation will be given to the individual without undue delay and at the latest within one month, informing them of their right to complain to the Information Commissioner's Office.

Time Limits

Legally, a formal request for Access to Records must be processed and completed within one calendar month. It is essential that any formal request for records be date-stamped with the date of receipt and actioned within a reasonable timeframe. A copy of the request should be filed on the customer's record.

5. Requests for Children and Young People Records

A person with parental responsibility can make a subject access request on behalf of their children who are too young to make their own request. Under GDPR, a young person aged 13 or above is generally considered competent enough to understand what a subject access request is. If they are judged competent to understand, they can make their own request and must provide their consent to allow their parents to make the request for them.

Parental Responsibility

It is important to ascertain parental responsibility before complying with any information requests. Not all parents have parental responsibility. Staff must verify this status before proceeding.

Competence Assessment

Staff must use their own judgement to decide whether a young person aged 13 or older is competent enough to make their own request, as they do not always have the maturity to do so.

Multiple Parental Responsibility

Where more than one person has parental responsibility, each may independently exercise rights of access. For example, if a child lives with their mother and the father applies for access to the child's records, there is no obligation to inform the child's mother that access has been sought. Access should only be given with the child's consent if the child is capable of giving consent.

Consent

If capable, an adult customer should be asked to give explicit consent to information about them being disclosed. A child of any age may also give such consent, provided they are sufficiently competent to understand the nature of the disclosure. If the child is not sufficiently competent, consent to disclose may be given by anyone with parental responsibility for them.

6. Requests Where the Customer is Deceased

Data protection laws apply only to living individuals. However, where the customer has died, their personal representative is entitled to apply for access to information about the deceased. A customer's personal representative is defined as:

- An executor appointed under the deceased's will.

- A person appointed as administrator where there is no will.

If the applicant is not a personal representative, dependents of a deceased customer may have a claim arising out of the death. Dependents are defined as including:

- The spouse or civil partner, or the former spouse or civil partner of the deceased.
- Any person who:
    - Was living with the deceased in the same household immediately before the date of death.
    - Had been living with the deceased in the same household for at least two years before that date.
    - Was living during the whole of that period as the spouse or civil partner of the deceased.
- Any parent or other ascendant of the deceased.
- Any person who was treated by the deceased as their parent.
- Any child or other descendant of the deceased (including an infant born after the death but who was conceived but not born at the time of the injury that caused the death).
- Any person (not being a child of the deceased) who, in the case of any marriage or civil partnership to which the deceased was at any time a party, was treated by the deceased as a child of the family in relation to that marriage or civil partnership.
- Any person who is, or is the issue of, a brother, sister, uncle, or aunt of the deceased.

7. Requests for Information by the Police

The Anthony Seddon Fund aims to maintain good relations with the police and contribute to public safety while also protecting customer confidentiality. Information about a customer, including the fact that they are a customer, is confidential and may only be disclosed under certain conditions.

Legal Compliance

The Anthony Seddon Fund must comply with GDPR and other data protection laws. Information may only be disclosed with the consent of the customer or in exceptional circumstances.

Exceptional Circumstances

Disclosures may be necessary in the public interest where a failure to disclose information may expose the customer or others to the risk of death or serious harm. Such circumstances may arise where disclosure is necessary for the prevention of serious crime, whether the customer is the victim or suspected of committing an offence. Each case must be considered individually.

Consent

- **Customer Consent**: If capable, an adult customer should be asked to give explicit consent to information about them being disclosed unless the police provide valid reasons why this would be detrimental to the investigation or prevention of a serious crime.
- **Child Consent**: A child of any age may give such consent if they are sufficiently competent to understand the nature of the disclosure. If the child is not sufficiently competent, consent may be given by anyone with parental responsibility for them.
- **Details of Consent**: Consent must be less than six months old and must detail to whom the information is being disclosed, what parts of the record are being disclosed, and why the information is requested.

Without Consent

If the consent of the customer cannot be obtained, the following principles apply:

- **Police Requests**: The police do not have a general right of access to records or information about customers. Unless there is a court order, the final decision about what may be disclosed rests with The Anthony Seddon Fund.
- **Serious Crime Prevention**: Disclosure of confidential information may be necessary for the prevention or detection of serious crime.
- **Police Officer Verification**: A police officer requesting disclosure of confidential information should provide:
    - Confirmation that the offence being investigated is a serious crime.
    - Reasons for believing the subject of the request has committed or is about to commit such an offence.
    - Reasons why the provision of the information requested will assist the investigation.
    - Explanation of urgency, if applicable.
- **Verification of Identity**: Anyone claiming to be a police officer should produce their warrant card, which includes:
    - The Greater Manchester Police logo.
    - The officer's photo.
    - Their warrant number.
    - A signature from the chief constable.
- **Verification of Request**: If there is any doubt about the request's validity, verification can be sought by contacting the police on 0161 872 5050. Requests received over the phone can also be verified at this number.

Disclosure of Information

Only information relevant to the police inquiry should be disclosed.

8. Request for Information from Solicitors

Requests for information from solicitors must be handled with care to ensure compliance with data protection laws and the confidentiality of customer information.

Written Requests

- **Formal Request**: Solicitors must submit a formal written request for information. This request should clearly state the purpose of the request and specify the information required.
- **Clarification of Intent**: Clarify whether the request is related to an action against The Anthony Seddon Fund. If so, this should be explicitly stated.

Right of Access

- **No Special Rights**: Solicitors have no greater right of access to information than their clients. They must provide the same proof of authority to act on behalf of the client as any other third party.
- **Client Authorisation**: The solicitor must provide written authorisation from the client, confirming that they have the client's permission to request and receive the information.

Verification

- **Verification of Solicitor Identity**: Verify the identity of the solicitor and the legitimacy of their request. This may involve contacting the solicitor's firm directly to confirm the request's authenticity.
- **Proof of Identity**: Ensure that sufficient proof of the client's identity and the solicitor's authorisation to act on the client's behalf is provided before releasing any information.

Handling Requests

- **Relevance of Information**: Only provide information relevant to the solicitor's request. Ensure that no additional, unnecessary information is included.
- **Confidentiality and Security**: Ensure that all information provided to solicitors is handled with the highest level of confidentiality and security. Follow the same protocols as for other sensitive data disclosures.

9. Sending the Record to the Applicant

Postal

- **Copies Only**: Only copies of records should be sent to any applicant. Under no circumstances must original records be removed from The Anthony Seddon Fund premises.
- **Sealed Envelope**: All access responses should be enclosed in a sealed, tamper-proof envelope clearly marked 'TO BE OPENED BY ADDRESSEE ONLY'.

- **Proof of Identity and Address**: Where the address of the customer is different from that shown on their records, proof of identity and address (e.g., a household bill or driving license) may be required before the records can be sent through the post.
- **Return Address**: A return address should be clearly marked on the reverse of the envelope in case of non-delivery. The best practice is to send records via special delivery.
- **Preferred Method of Delivery**: Clarify with the data subject whether they would prefer the records to be sent via post (special delivery), email, or collected in person.

Records Collected in Person

- **Proof of Identity**: Where an access response is to be collected personally by the applicant, positive proof of identity must be provided before such information is released if the applicant is unfamiliar.
- **Sign for Records**: The records must be signed for, and the date collected should be recorded.

Email

- **Encryption**: When sending records via email, use encryption to ensure the security and confidentiality of the information.
- **Verification of Email Address**: Verify the email address with the applicant to ensure accuracy.
- **Password Protection**: Attachments containing personal information should be password-protected. The password should be sent via a separate communication method (e.g., text message or phone call).
- **Confirmation of Receipt**: Request a confirmation of receipt from the recipient to ensure that the email has been received securely.

10. Data Subject Rights

Under the General Data Protection Regulation (GDPR) and other data protection laws, individuals are granted the following rights regarding their personal data:

The Right to Be Informed

Individuals have the right to be informed about the collection and use of their personal data. The Anthony Seddon Fund must provide clear and concise information about why personal data is being processed, how it is used, and with whom it is shared.

The Right of Access

Individuals have the right to access their personal data and supplementary information. This enables individuals to be aware of and verify the lawfulness of the processing. Subject Access Requests (SARs) should be processed in accordance with the procedures outlined in this policy.

The Right to Rectification
Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete. If the Anthony Seddon Fund has disclosed the personal data to others, it must contact each recipient and inform them of the rectification, unless this proves impossible or involves disproportionate effort.

The Right to Erasure
Also known as the 'right to be forgotten,' individuals have the right to have their personal data erased if:

- The data is no longer necessary for the purpose for which it was collected.
- The individual withdraws consent (where consent was the legal basis for processing).
- The individual objects to the processing, and there is no overriding legitimate interest in continuing the processing.
- The data was unlawfully processed.
- The data must be erased to comply with a legal obligation.
- The data was processed in relation to the offer of information society services to a child.

The Right to Restrict Processing
Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, the Anthony Seddon Fund is permitted to store the personal data but not use it. This right applies if:

- The accuracy of the data is contested by the individual.
- The processing is unlawful, and the individual opposes erasure.
- The Anthony Seddon Fund no longer needs the data, but the individual requires it to establish, exercise, or defend a legal claim.
- The individual has objected to the processing, and the Anthony Seddon Fund is considering whether its legitimate grounds override those of the individual.

The Right to Data Portability
Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This right allows them to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure manner without hindrance to usability.

The Right to Object
Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest or the exercise of official authority (including profiling).
- Direct marketing (including profiling).
- Processing for purposes of scientific or historical research and statistics.

The Anthony Seddon Fund must stop processing personal data unless it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual, or for the establishment, exercise, or defence of legal claims.

Rights in Relation to Automated Decision-Making and Profiling
Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. Exceptions apply if the decision:

- Is necessary for entering into or performing a contract between the individual and the Anthony Seddon Fund.
- Is authorised by law (e.g., for the purposes of fraud or tax evasion prevention).
- Is based on the individual's explicit consent.

11. Dealing with Complaints

The Anthony Seddon Fund is committed to addressing any complaints regarding access to records promptly and effectively. This section outlines the process for handling such complaints.

Informal Resolution

- **Initial Contact**: If a customer is unhappy with the outcome of their request for access to records, they should initially contact the General Manager for further guidance.
- **Informal Meeting**: The General Manager may arrange an informal meeting with the individual to discuss their concerns and attempt to resolve the complaint locally. This meeting aims to understand the issue and provide an immediate resolution where possible.

Formal Complaints Procedure
If the complaint cannot be resolved informally, the customer should be advised to follow the formal complaint procedure as outlined in **HR-002 - Complaints Policy**. The steps for a formal complaint are as follows:

- **Written Complaint**: The customer should submit a written complaint detailing their concerns and the specific issues they have encountered.
- **Acknowledgement**: Upon receipt of the formal complaint, the General Manager will acknowledge the complaint in writing within five working days.
- **Investigation**: The General Manager or a designated investigator will conduct a thorough investigation into the complaint. This may involve reviewing the original request, the handling of the request, and any relevant communications.
- **Resolution**: Following the investigation, the General Manager will provide a written response to the complainant within 20 working days. This response

will include the findings of the investigation and any actions taken to address the complaint.

Escalation

If the complainant is not satisfied with the outcome of the formal complaint procedure, they have the right to escalate the matter. The steps for escalation are as follows:

- **Review by Trustees**: The complainant can request that the matter be reviewed by the Board of Trustees. The Trustees will consider the complaint and the investigation findings and provide a final decision.
- **External Review**: If the complainant remains dissatisfied, they may refer the complaint to an external body, such as the Information Commissioner's Office (ICO).

Data Protection Officer (DPO) Involvement

The DPO will be informed of all formal complaints related to access to records and will provide advice and support throughout the investigation process to ensure compliance with GDPR and other data protection laws.

12. What if Corrections or Erasures Are Requested?

Individuals have the right to request that any inaccurate or incomplete personal data held about them be corrected or erased. The Anthony Seddon Fund is committed to ensuring that personal data is accurate and up-to-date. This section outlines the process for handling such requests.

Corrections

- **Request for Correction**: If an individual believes that any information contained in a record is inaccurate, they may apply for the necessary corrections to be made. This request should be submitted in writing to the General Manager.
- **Review of Request**: The record holder will review the request and determine whether the information is indeed inaccurate.
- **Making Corrections**: If the record holder is satisfied that the information is inaccurate, the necessary corrections will be made. The correction should be signed and dated by the record holder and the applicant. A copy of the corrected record will be provided to the applicant free of charge.
- **Disputes**: If the record holder is not satisfied that the information is inaccurate, they will discuss the alleged inaccuracy with the customer and document the discussions. The customer's request and the record holder's response will be recorded in the file.

Erasures

- **Request for Erasure**: If an individual wishes to have their personal data erased, they should submit a written request to the General Manager. The

request should specify the data they wish to be erased and the reasons for the request.

- **Review of Request**: The General Manager will review the request to determine if the data meets the criteria for erasure under GDPR, such as:
    - The data is no longer necessary for the purpose for which it was collected.
    - The individual withdraws consent (where consent was the legal basis for processing).
    - The data was unlawfully processed.
    - The data must be erased to comply with a legal obligation.
- **Erasure Process**: If the data meets the criteria for erasure, the General Manager will ensure that the data is erased from all relevant systems and records. The erasure should be documented, and the individual will be informed in writing that the data has been erased.
- **Disputes**: If the General Manager determines that the data does not meet the criteria for erasure, the individual will be informed in writing of the decision and the reasons for it. The individual has the right to contest this decision and seek further review.

Documentation and Transparency

- **Record Keeping**: All requests for corrections or erasures, along with the decisions and actions taken, will be documented and kept on file. This ensures transparency and accountability in the handling of such requests.
- **Providing Copies**: The applicant must be provided, without charge, with a copy of the corrected record or a note of the request and the discussions if the correction is not made.
- **Non-obliteration**: When corrections are made, care must be taken not to obliterate information. It is recommended that a single line be drawn through the error, with the correction dated and signed. The use of obliterating material (e.g., Tippex) must never be used.

If the individual is not satisfied with the outcome of their application for correction or erasure, they can make a complaint via the charity's complaints procedure as outlined in **HR-002 - Complaints Policy**.

13. Review

This policy will be reviewed annually to ensure that it remains up-to-date and reflects the needs and practices of the organisation.

The policy may also be reviewed if legislation changes or if monitoring information suggests that policy or practices should be altered.