Data Protection Policy (GDPR)

Raise is committed to a policy of protecting the rights and privacy of individuals, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how charities manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use. The GDPR contains provisions that RAISE will need to be aware of as data controllers, including provisions intended to enhance the protection of client's personal data. For example, the GDPR requires that: We must ensure that our privacy notices are written in a clear, plain way that staff and clients will understand.

1. Compliance

This policy applies to all staff and volunteers of Raise. Any breach of this policy or of the Regulation itself will be considered an offence and Raise's disciplinary procedures will be invoked. As a matter of best practice, other agencies and individuals working with Raise and who have access to personal information, will be expected to read and comply with this policy. It is expected that partners/funders sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

2. General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an

individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO). Please follow this link to the ICO's website (www.ico.gov.uk)

3. Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found in the DPCoP. Please follow this link to the ICO's website (www.ico.gov.uk) In order to comply with its obligations, RAISE undertakes to adhere to the eight principles:

1) Process personal data fairly and lawfully.

RAISE will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

RAISE will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

RAISE will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4) Keep personal data accurate and, where necessary, up to date.

RAISE will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify RAISE if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of RAISE to ensure that any notification regarding the change is noted and acted on.

5) Only keep personal data for as long as is necessary.

RAISE undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means RAISE will undertake a regular review of the information held and implement a archiving and destroying process. RAISE will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6) Process personal data in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information RAISE holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened. RAISE will only process personal data in accordance with individuals' rights.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. RAISE will ensure that all personal data is accessible only to those who have a valid reason for using it. RAISE will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- keeping all personal data in a lockable cabinet with key-controlled access.
- password protecting personal data held electronically.
- archiving personal data which are then kept securely (lockable cabinet).
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.
- Members of staff and clients will be offered a private place to discuss information of a personal or confidential nature

In addition, RAISE will put in place appropriate measures for the deletion of personal data - manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and volunteers who process personal data 'off-site', e.g. when working at home, or on home visits and in circumstances additional care must be taken regarding the security of the data. Please see RAISE Home Working Policy for further detailed information.

8) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

RAISE will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so BCA will always seek the consent of individuals before placing any personal data (including photographs) on its website. If RAISE collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

4. Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when RAISE is processing any sensitive data, as defined by the legislation. RAISE understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via the authority form for clients or this data protection policy for staff and volunteers) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Personal Details

- For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to RAISE holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in RAISE's data protection policy.

- This will include marketing images." RAISE will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

5. Personal data

The Regulations provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- that data

- that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- criminal proceedings or convictions.

6. How We Use Your Personal Information

In order for RAISE to carry out its Charitable Aims we need to process certain information about its staff, clients, volunteers and other individuals with whom it has a relationship for various purposes (past and present) such as, but not limited to:

1. The recruitment and payment of staff.

2. Giving advice to client and pursue their case.

3. The administration of programmes of training and courses.

4. Recording client case management progress, success and gains.

5. Providing monitoring information example anonymous statistics about the ethnic origin for staff, volunteer and client personal and sensitive data.

6. Complying with legal obligations to funding bodies and government including local government.

Information may be shared with third parties for financial, monitoring, training, employment and well-being related purposes. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 1998. Raise will not attempt to gain information that is not necessary to hold.

7. Data management

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR), RAISE must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Personal information relating to clients, employees, job applicants, volunteers will be held for a period in accordance with Raise's Document Retention Policy**,** after which it will be destroyed.

Anonymous information will be retained for monitoring purposes, e.g. equal opportunities statistics.

8. Data Security

Personal information relating to clients, employees, job applicants, volunteers will be kept securely within the RAISE Office which operates a clear desk policy.

The Clear Desk policy means that all client or employee personal and sensitive data will be stored in locked draws or filling cabinets unless actively working with the paperwork.

Our electronic system is secure as per our Comprehensive Confidentiality and ICT Security Policy as well as all our computer monitors being password protected within the office as well as due authentication when accessing externally.

9. Data Communication

Individuals will be made aware of the reasons why personal information is required and held and their right to access it within our Privacy Policy/Notice.

10. Responsibilities under the GDPR

RAISE will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The Chief Officer is available to address any concerns regarding the data held by RAISE and how it is processed, held and used. RAISE also has a nominated Board Director who oversees this policy. The Leadership Team is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within RAISE.

Compliance with the legislation is the personal responsibility of all members of RAISE who process personal information. Staff and volunteers who provide personal data to the RAISE are responsible for ensuring that the information is accurate and up-to-date.

11. Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by RAISE. Any individual wishing to exercise this right should apply in writing to the Chief Officer. Any member of staff receiving a SAR should forward this to the Chief Officer without delay. Under the terms of the legislation, any such requests must be complied with within 30 days. For a detailed policy on responding to SARs see **appendix one.**

12. Disclosure of Data

Only disclosures which have been detailed in appendix one must be made and therefore staff and volunteers should exercise caution when asked to disclose personal data held on another individual or third party. RAISE undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the Police.

Legitimate disclosures may occur in the following instances:

- The individual has given their consent to the disclosure.

- The disclosure has been notified to the ICO and is in the legitimate interests of RAISE.
- The disclosure is required for the performance of a contract.
- Child or Adult safeguarding when there is serious risk of harm.

There are other instances when the legislation permits disclosure without the consent of the individual.

13. Publication of RAISE Information

RAISE publishes/shares various items which will include some personal data, e.g.

- internal telephone directory
- emergency numbers
- birthday list
- photos and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted RAISE access only. Therefore it is our policy to offer an opportunity to opt-out of the publication of such when collecting the information.

14. Staff and volunteer training and awareness

Raise's Chief Officer will ensure that all staff and volunteers have received the appropriate training and learning to meet the data protection regulations. Managers and team leaders will be responsible for ensuring that staff comply with this policy and that:

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or volunteer or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

Staff and volunteers will be responsible for informing their team leader or the data controller if they are aware of a breach of this policy.

Staff and volunteers will be made aware of the policy via the staff handbook

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998. Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website. For help or advice on any data protection or freedom of information issues, please do not hesitate to contact the Chief Officer.

ICO registration

Our data protection registration number is Z9387448.

Policy Review

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the Chief Officer.

Author:	Alan Bornat, Manager	**Date:**	
Review	Emma Cook, Chief Officer	**Date:**	July 2018
Approved by:	Board of Trustees	**Date:**	25 July 2018
Review	Emma Cook, Chief Officer	**Date:**	November 2019
Approved by:	Board of Trustees	**Date:**	13 November 2019
Review	Emma Cook, Chief Officer	**Date:**	November 2020
Approved by:	Board of Trustees	**Date:**	December 2021
Review	Penny Brown, Chief Officer	**Date:**	May 2023
Approved by:	Board of Trustees	**Date:**	17 May 2023
Review	Manager Linda Daley	**Date:**	8 May 2025
Approved by:	Board of Trustees	**Date:**	21 May 2025
Next review	May 2027		

Appendix one

Subject Access Rights (SARs) Policy

Introduction and applicability

Individuals have the right superseded by the General Data Protection Regulation (GDPR) 2018, subject to certain exemptions, to have access to their personal records that are held by RAISE Ltd. This is known as a 'subject access request' (SAR).

Requests may be received from members of staff, clients or any other individual who the RAISE has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, audio recordings etc.

Anyone making such a requested is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, where the information was gathered from.

Under GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or Raise and objection to the processing altogether.

The Data Protection Act 1998 (and GDPR) applies only to living persons but there are limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990.

Raise has developed this policy to guide staff in dealing with Subject Access Requests that may be received.

The aim of this policy is to inform staff on, how to advise clients on how to make a subject access request, how to recognise a subject access request and know what action to take on receipt.

This procedure sets out the processes to be followed to respond to a subject access request. This is based on the Information Commissioner's Office Subject Access Code of Practice: ICO Subject Access Code of Practice.

Policy purpose and aims

What is a Subject Access Request?

A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information about them, which is held by RAISE. General Data Protection Regulation (GDPR) entitles all individuals to make requests for their own personal data. An individual is not entitled to information relating to other people (unless they are acting on behalf of that person). The request does not have to be in any particular form other than in writing, nor does it have to include the words 'subject access' or make any reference to the Data Protection Act 1998 or the General Data Protection Regulation (GDPR) 2018. A SAR may be a valid request even if it refers to other legislation, such as the Freedom of Information Act 2000 (FOIA) and should therefore be treated as a SAR in the normal way. The applicant must be informed of how the application is being dealt, under which legislation and of any fees applicable. Where an individual is unable to make a written request it is the

RAISE's view that in serving the interest of the client it can be made verbally, with the details recorded on the individual's file.

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

Personal data is information that relates to an individual who can be identified either directly or indirectly and includes any expression of opinion about the individual and any indication of the intentions of the information holder or any other person in respect of the individual. Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR.

- Information supplied by third parties.
- Data and information held from other agencies may be disclosable but should be discussed with the originating body first.
- Any information subject to Legal Professional Privilege should not be disclosed.
- Information should not be disclosed where there is a statutory or court restriction on disclosure e.g. adoption records.
- References written for current or former employees are exempt (but not those received from third parties).
- In the case of deceased records, information should not be disclosed where the entry in the records makes it clear that the deceased expected the information to remain confidential.
- A personal record may also contain reference to third parties and redaction should be considered by balancing the Data Protection rights of all parties.

How to recognise and action a Subject Access Request

In order for RAISE to action a subject access request the following must be received:

- The request must be made in writing (This may be by letter, fax, email, or even social media, such as Facebook or twitter). It is important to note that responses to SAR requests must be returned by a secure methodology, i.e. social media must NOT be used to return information requested. However where the applicant is not able to make the request in writing it can be received verbally and a record of the request made on the applicants file or it can be written in their file.

- Proof of identity of the applicant and/or the applicant representative, and proof of right of access to another person's personal information.
- Sufficient information to be able to locate the record or information requested. Requests should be dealt with within a calendar month. It is possible to extend this timescale by a further two months where requests are complex. However if this is the case RAISE must inform the individual within one month of the request and explain why the extension is necessary.

All SAR requests received must be forwarded to your line manager or a manager, without delay in order for it to be processed within the legal timescale.

Assisting and advising client on how to make a request

Where an individual is verbally making a request you should advise that the will need to:

- Put the request in writing, detailing the information they are requesting and from which service to enable it to be located. (Send them the form).
- Requesters do not have to tell you their reason for making the request or what they intend to do with the information requested, although it may help you to find the relevant information if they do explain the purpose of the request.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure that you and your colleagues can recognise a SAR and deal with it in accordance with this procedure and forward immediately to your line manager or a manager.
- In order to comply with equality legislation, where an applicant is unable to put the request in writing assistance should be given to them to make the request verbally, best practice would be to document the request details in an accessible format for the applicant and request them to confirm the details are correct. Please speak to your line manager or manager about this.
- Note that responses to requests should be made in a format requested by the applicant, therefore alternative formats may be needed.

Requests made about or on behalf of other individuals

General Third Party

A third party, e.g. solicitor, may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g. power of attorney must be provided by the third party.

If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

Access Requests for those who lack capacity to consent

In certain circumstances a person acting as an advocate can seek access to personal information in so far as it is necessary or relevant to their role. This includes;

- Persons appointed by the Court of Protection.
- Persons holding a registered Power of Attorney for specified purposes.
- Persons appointed as Independent Mental Health Advocates under the Mental Capacity Act 2005.

Remote Access to Records

• Under GDPR, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to their information.

• The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

We don't currently have an systems that would allow this.

Court Orders

Any Court Order requiring the supply of personal information about an individual must be complied with.

Responding to requests

The Collection: It is essential that a log of all requests received is maintained, detailing:

- Date received.
- Date response due (maximum of one month under GDPR).
- Applicants details.
- Information requested.
- Exemptions applied in respect of information not to be disclosed.
- Details of decisions to disclose information without the data subjects consent.
- Details of information to be disclosed and the format in which they were supplied.
- When and how supplied, e.g. paper copy and postal method used to send them.

Determine whether the person's request is to be treated as a routine enquiry or as a subject access request. If you would usually deal with the request in the normal

course of business, e.g. confirming appointment times or updating them on a case. Then please continue to do so.

The following are likely to be treated as formal subject access requests.

- *Please send me a copy of my HR file.*
- *I am a solicitor acting on behalf of my client and request a copy of his medical records. An appropriate authority is enclosed.*
- *The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior officer.*

Ensure adequate proof of the identity of both the data subject and the applicant, where this is a third party is obtained before releasing information requested, this may be in the form of documentation as detailed at Annex A.

Ensure adequate information has been received to facilitate locating the information requested.

Pass the information to your Team Leader. The Team Leader will Locate the required information from all sources and collate it ready for review by The Chief Officer

The Review

The Chief Officer will review the paperwork. This review is to ensure that the information is appropriate for disclosure, i.e. to ascertain whether any exemptions apply e.g. it does not contain information about other individuals, it is likely to cause harm or distress if disclosed, or is information to be withheld due to on-going formal investigations.

Where information in respect of other individuals is contained within the information requested it should not be disclosed without the consent of that individual.

Where it is ascertained that no information is held about the individual concerned, the applicant must be informed of this fact.

It must be determined whether the information is likely to change between receiving the request and sending the response. Routine on-going business additions and amendments may be made to the personal information after a request is received, however the information must not be altered as a result of receiving the request, even if the record contains inaccurate or embarrassing information, as this would be an offence under the General Data Protection Regulation (GDPR) on 25th May 2018.

Check whether the information collated contains any information about any other individuals and if so, consider:

Is it possible to comply with the request without revealing information that relates to the third party? (Ensure that consideration is given what information the requestor may already have or get hold of that may identify the third party) Where it is not possible to remove third party identifiers you must consider the following.

- Has the third party consented to the disclosure?

- Is it reasonable, considering all the circumstances, to comply with the request without the consent of the third party? (The following must be considered when trying to determine what reasonable circumstances are);
- duty of confidence owed to the third party,
- steps taken to try and obtain consent,
- whether the third party is capable of giving consent, and
- any express refusals of consent from the third party.

A record of the decision as to what third party information is to be disclosed and why should be made.

Consider whether you are obliged to supply the information, i.e. consider whether any exemptions apply in respect of:

- Crime prevention and detection, including taxation purposes,
- Negotiations with the requestor,
- Management Forecasts,
- Confidential References given by you,
- Information used in research, historical or statistical purposes; and
- Information covered by legal professional privilege.

Other exemptions are detailed at Annex D. If the information requested, is held by the organisation and exemptions apply then a decision must made as to whether you inform that applicant that the information is held but is exempt from disclosure or whether you reply stating that no relevant information is held. A response in these circumstances must be carefully considered and applied as appropriate giving due consideration to the exemptions being applied as it may be appropriate to deny holding information if prejudicing on-going or potential investigations or undue harm or distress is to be avoided.

NB. It may be necessary to reconsider this decision should a subsequent application be made and circumstances around the use of exemptions has altered.

If the information contains complex terms, you must ensure that these terms are explained in such a way that the information can be understood in lay terms.

Preparing the response:

- When the requested information is not held, inform the applicant in writing, as soon as possible, but in any case by the due date.

A copy of the information should be supplied in a permanent form except where the individual agrees or where it is not possible in the format requested or would involve undue effort. This could include very significant cost or time taken to provide the information in hard copy form.

You have a maximum of one month under GDPR to comply with the request starting from the date you receive all the information necessary to deal with the request. It is

an offence under the GDPR and individuals can complain to the Information Commissioners Office or apply to a court if you do not respond within this time limit.

NB Under no circumstances should original records be sent to the applicant.

Ensure that the information to be supplied is reviewed by another senior manager and written authorisation and / or agreement of exemptions applied is obtained for disclosure or non-disclosure of the information.

Implementation

The policy will be disseminated by being made available on the server within the policy and procedure folder.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under RAISE's disciplinary procedure'.

Training and awareness

Staff and volunteers will be made aware of the policy via the shared files and the policy is one of the Priority Policies of the organisation, requiring staff and volunteers to read the policy annually.

Policy Review

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the Chief Officer.

Author:	Alan Bornat, Manager	**Date:**	
Review	Emma Cook, Chief Officer	**Date:**	July 2018
Approved by:	Board of Trustees	**Date:**	25 July 2018
Review	Emma Cook, Chief Officer	**Date:**	November 2019
Approved by:	Board of Trustees	**Date:**	13 November 2019
Review	Emma Cook, Chief Officer	**Date:**	November 2020
Approved by:	Board of Trustees	**Date:**	December 2021
Review	Penny Brown, Chief Officer	**Date:**	May 2023
Approved by:	Board of Trustees	**Date:**	17 May 2023

Review	Manager Linda Daley	**Date:**	8 May 2025
Approved by:	Board of Trustees	**Date:**	21 May 2025
Next review	May 2027		

Subject Access request form

Please complete this form if you want RAISE to supply you with a copy of any personal or sensitive data we hold about you.

We will only use the details in this form for the purpose of identifying the personal data we hold on you. We will keep a copy of this form and any correspondents and personal data disclosed for a period of 6 years.

Once we have received the form we will respond within one calendar month. If for some reason we are not able to do this we will write to you to advise you of the delay, the reasons for the delay and the likely time scale.

There are some circumstances under Data Protection legislation that allows RAISE to withhold information.

For example where information we hold is likely to cause serious harm to your physical or mental wellbeing or another person. In addition if we have information relating to a third person who has not consented to the disclosure.

		Yes	No	Comments
1.	Is the personal data that you have requested about you as an individual? (we can only except request from the individual concerned unless point 3 applies.)			
2.	Have you provided evidence of your identity e.g. photocopy of passport, driving licence, birth certificate or marriage certificate			
	I am the individual concerned but I am acting on their behalf as their parent or legal guardian and enclose evidence of their identity e.g. photocopy of birth certificate, passport			

I am NOT the Data Subject, but I am acting on their behalf as their parent or legal guardian and enclose evidence of their identity e.g. photocopy of birth certificate, passport. ☐

Section 2

Details of the Data Subject:

Full Name	
Former Names(s)	
Current address (including postcode)	
Former address(s)	
Date of birth	
Contact telephone number (including area code)	
Email address	
Any additional information that may help identify your relationship with RAISE	

Section 3

Details of representative (please complete this section if you are NOT the data subject, but are authorised to act on their behalf)

Full Name	
Former Names(s)	
Current address (including postcode)	
Former address(s)	
Date of birth	
Contact telephone number (including area code)	
Email address	
Relationship with the data subject that leads you to make this request for information on their behalf	

Section 4

What service have you received from RAISE? Employee past or present Volunteer past or present clients for Debt/ Client for Benefits Client for Financial Capability Other	
What information would you like from us?	
Anything further that you wish to tell us?	
Please now send this form back to: Chief Officer **RAISE** 107 Great Mersey Street Liverpool L5 2PL Email admin@raiseadvice.org.uk	