General Data Protection Procedures

Owner	**Phoebe Pham, Office Manager**
Author	**Phoebe Pham, Office Manager**
Date approved by SMT	
Version	**1.0**
Date last reviewed	
Date of next review	**June 2027**
Changes from previous version	

1. PURPOSE AND SCOPE

1.1 This procedure is designed to operationalise Action Foundation (the Charity) commitment to protecting personal data, in compliance with the UK General Data Protection Regulation (UK GDPR). The aim is to:

- Support our data protection principles
- Protect data subjects' privacy rights
- Reduce the risk of data breaches.
- Ensure staff and volunteers follow consistent, compliant data handling practices.

1.2 It applies to all individuals worked, volunteered and engaged with the organisation. This procedure document should be read alongside the following documents:

- GDPR policy
- Privacy Notice
- IT security Policy
- Complaints Policy
- Grievance Procedure
- Whistleblowing Policy

2. DATA PROCESSING ACTIVITY PROCEDURES

2.1 Acting as a Data Controller

When operating as a Data Controller, the Charity is committed to ensuring that all personal data and associated processing activities are clearly documented in accordance with Article 30 of the UK GDPR.

Managers are designated by the Charity to support the following:

- Identifying and accurately documenting all relevant data processing activities within the supervised service area.
- Notifying the Data Project Lead of any changes updated to the existing Record of Processing Activities (RoPA).

Note that the Charity retains ultimate responsibility.

2.2 Acting as a Data Processor

When acting as a Data Processor on behalf of an external Data Controller, the Charity is committed to supporting the terms of the data processing agreement, provided they align with UK GDPR requirements.

Each manger must:

- Where applicable, forward the Data Processing Agreement (DPA) to the Data Protection Lead (DPL) or Senior Managers for review, approval, and record-keeping. Managers may only sign DPAs if explicitly authorised by the DPL or a senior manager, to ensure alignment with the Charity's data protection policies and UK GDPR requirements.

- Promptly alert the DPL to any actual or potential conflicts between the DPA and the Charity's General Data Protection Policy or procedures and support the resolution process.
- Ensure full compliance with the terms of the agreement.

2.3 Maintenance of Data Processing Activity Records (RoPA)

All managers are responsible for maintaining accurate, completing, and up-to-dating records of processing activities within their service areas.
Any updates or additions to processing activities should be communicated promptly to the DPL.

The DPL will conduct periodic reviews of RoPA entries and implement appropriate monitoring processes to ensure ongoing GDPR compliance.
Upon request, the DPL will provide the current RoPA to the Senior Management Team (SMT).

3. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

3.1 The Charity will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

3.2 The Charity must ensure that DPIAs are conducted in respect to high-risk processing. DPIAs will be conducted by managers who must then update the RoPA and discuss findings with the DPL.

3.3 A DPIA should be conducted when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and automated decision-making;
- large scale processing of special categories of personal data or criminal convictions data; and
- large scale, systematic monitoring of a publicly accessible area (e.g., CCTV or surveillance in public areas).

3.4 A DPIA must include:

- a description of the processing operations and the purposes
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

4. DATA SHARING AND DISCLOSURE

4.1 The Charity recognises its obligation to handle personal data lawfully, fairly, and transparently. No personal data shall be disclosed or shared unless permitted under the UK GDPR, and where appropriate, subject to internal controls, risk assessments, and documented agreements.

4.1.1 Lawful Basis for Sharing Data

Before sharing personal data, it is important to ensure that:

- A lawful basis for processing under Article 6 of the UK GDPR applies.
- If the data involves Special Category Data, an additional condition under Article 9 is required.
- Where practical, individuals should be informed through a Privacy Notice explaining the relevant legal basis and purpose for processing.

For guidance, refer to the Charity's GDPR Policy for a summary of Articles 6 and 9.

4.1.2 Internal Sharing of Personal Data

Where possible, internal access should be proportionate and clearly linked to the purpose for which the data was collected. Internal sharing should be limited to what is necessary:

- Sharing must be strictly limited to employees, casual workers, contractors, volunteers with a legitimate need to know in order to fulfil their duties.
- Special care must be taken with Special Category Data, ensuring it is handled securely and shared only when essential.
- All employees, casual workers, contractors, volunteers must adhere to internal data access protocols and confidentiality obligations.

4.1.3 External Sharing of Personal Data

Sharing data with external parties must follow a structured process to ensure compliance and accountability:

a) Permissible Circumstances

Data must not be shared routinely unless:

- It is governed by an existing, documented Data Sharing Agreement (DSA) or contract.
- The sharing is required by law or regulation.
- Approval has been obtained from the DPL.

b) Due Diligence

Before sharing externally, all individuals must:

- Ensure that the data type and purpose fall within the scope of the DSA or legal requirement.
- Assess whether the receiving organisation meets appropriate data protection standards.
- Ensure that no conflict exists between the DSA terms and the Charity's internal GDPR policies. Any discrepancies must be reported to the DPL.

c) Documentation and Risk Assessment

- All external sharing should be formally documented.
- A Data Protection Impact Assessment (DPIA) should be considered prior to sharing and is mandatory where the processing poses a high risk to individuals' rights and freedoms.
- In a case where high risk cannot immediately be ruled out, a DPIA should be carried out as this is the best way to assess the level of risk.

While formal review or documentation may not be necessary in every case, it is advisable to consult the DPL if there is any uncertainty. The DPL can also provide support in coordinating Data Protection Impact Assessments (DPIAs) or reviewing external data sharing arrangements where appropriate.

5. DATA SECURITY

The Charity will keep personal data secure by taking appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage. Please refer to IT security policy and procedure for detailed guidance.

6. DATA RETENTION AND DISPOSAL

6.1 Retention Schedules

Personal data must only be retained for as long as necessary for the purposes for which it was collected, in line with UK GDPR principles. Most records lose their value over time and should be securely destroyed once their retention period ends.

Retention periods for all core data processing activities are documented in the RoPA, which should be consulted for reference.

Retention arrangements for digital records must ensure that files remain intact, accessible, and secure for the full duration of the retention period. During that period, records may be stored across different media or locations, but they must be managed in accordance with this policy.

6.2 Secure Disposal

Records should be reviewed as soon as possible after the expiry of the retention period. It need not be a detailed or time-consuming exercise but there must be a considered appraisal of the contents of the record. A record should not be destroyed without verification that:

- no work is outstanding in respect of that record and it is no longer required by any department within the Charity;
- the record does not relate to any current or pending complaint, investigation, dispute or litigation;
- the record is unaffected by any current or pending request made under UK GDPR.

All disposal decisions should be documented, and the destruction of records should be conducted in a manner that ensures the confidentiality of the information. All copies of a record, regardless of format, must be destroyed simultaneously. For detailed guidance on secure data disposal and destruction, refer to the IT Security Policy and associated procedures.

7. Handling of Individual Rights Requests

7.1 Data subjects can raise requests in relation to their individual data rights. Under UK GDPR, data subjects have the following rights:

- Right of access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling

7.2 Submitting a Request

7.2.1 Employees and Casual Workers as data subjects

Employees and casual workers can submit a request regarding their individual data rights by contacting either a member of the Human Resources (HR) department or the DPL.

7.2.2 Volunteers, Clients, Contractors, Applicants, and Other Individuals as data subjects

All other data subjects can choose to submit a rights request through one of the following methods:

- By contacting the relevant projects or departments. The employee monitoring mailboxes or calls will log the request and support its handling, responding the request appropriately.
- By making a verbal request to a relevant project or departmental employee, who must then record, handle and response.
- By submitting a written request directly to the DPL.

Appropriate contacts are as listed in Annex 1.

7.3 What to Do After Receiving a Data Subject Request

Upon receiving a data subject request, it is essential to determine the Charity's role with respect to the personal data involved in the request.

- If the Charity is acting as a data processor or a joint controller, any action in response to the request must be carried out in accordance with the relevant Data Processing Agreement (DPA) or any other documents that outlines these arrangements in place with the other party.
- If the Charity is the sole data controller, it is responsible for handling the request in line with its policies. The Charity's employees and its data processors must follow proper procedures and should treat the following steps as standard practice.

7.3.1 **Step1: Acknowledge**

Data subjects should receive an acknowledgment of their request **within five working days** of submission. This should include the expected response timeframe—usually within one calendar month from the date the request is received and identity verified. For complex or multiple requests, this may be extended by up to two additional months, with reasons provided.

Each request must be recorded, including the date received, requester's identity, and the assigned staff member.

7.3.2 **Step2: Verify the Data Subject's Identity**

Before any personal data is disclosed, it is essential to confirm the identity of the individual making the request. This is to prevent unauthorised access to personal information.

If the requester is already known to the organisation (e.g., an employee using a verified internal email,), no additional identity verification may be required. However, if there is any doubt, proof of identity must be requested. Here are examples of acceptable documents.

Proof of Name	Proof of Address
Valid UK passport	Utility bill (last 3 months)
UK birth certificate	Council tax bill (current year)
UK Photo-card Driving Licence	Bank/building society statement (last 3 months)
Valid Biometric Residence Permit/ An Application Registration Card	Mortgage statement (last full year)/ Valid Tenancy Agreements
Share code to check e-visa or documents confirming identity from Home Office	HMRC tax letter (current financial year)

Note that the response timeframe will be paused until the requester's identity has been verified.

7.3.3 **Step 3: Assess the Request:**

The request will be reviewed to determine which right is being exercised and whether the request is valid and clear.

If the request lacks sufficient detail, further contact to the requester is required to ask for clarification. This is particularly important for complex requests, where the data subject may need to specify particular data or time periods.

7.3.4 **Step 4: Locating and Reviewing the Data**

Necessary steps should be taken to locate and retrieve the personal data relevant to the request. This includes conducting a thorough search of all systems, databases, and filing records where personal data might be stored.

When reviewing the collected information, it's necessary to carefully consider whether any data needs to be redacted or withheld to protect the rights of third parties. Personal data should not be disclosed if doing so could negatively impact the rights and freedoms of others, including maintaining the confidentiality of third-party information.

Furthermore, any exemptions under the UK GDPR will be carefully evaluated in relation to the request. These exemptions may cover areas such as legal enforcement, national security or other sensitive matters.

When necessary, guidance will be sought from the DPL or legal advisors to ensure full compliance.

7.3.5 **Step 5: Engaging with Data Processors or Joint Controllers**

Reasonable efforts should be made to notify other controllers or processors if a data subject exercises any of their data rights related to data they hold.

- When acting as a data controller: If any data processors are involved with the data covered by the request, they must be notified promptly to support compliance.
- When acting as a data processor: Requests must be forwarded promptly to the data controller, and all actions must comply with the relevant Data Processing Agreement.
- When acting as a joint controller: Coordination with the other controller(s) must be carried out in accordance with the joint controller agreement.

7.3.6 **Step 6: Responding to the Request**

The requested information should be provided in a clear, secure, and accessible format. If the request was submitted electronically, the response will be delivered electronically, unless the data subject requests otherwise.

The response should include:

- A copy of the personal data requested (where applicable).
- An explanation of how the data is processed.
- Information on the data subject's rights
- how to lodge a complaint with the ICO.

The data must be provided within stated timeframe. If an extension is required, the individual will be notified in advance with a justification.

7.3.7 **Step 7: Keep Records:**

All requests must be properly documented. This includes:

- Details of the request and the requester.
- Copies of identification provided.
- Notes on searches conducted and data reviewed.
- Any redactions or exemptions applied.
- All internal and external communications.
- The final response issued.

7.4 **Requests made by someone on behalf of someone else**

Individual requests made by someone other than the data subject should be approached with caution. Personal data should not be released unless it is clear that the person making the request has the authority to act on behalf of the person the personal data is about. For example, if a solicitor makes a request on behalf of their client then it will be necessary to ask for the signed authority of their client.

Children can make their own requests if they have capacity and understanding to do so. The age at which they have sufficient capacity and understanding will vary and be affected by any special educational needs they have which would affect their level of understanding. The capacity of a child should be assessed on an individual basis. If a child has capacity, then they should make their own request but if a parent, guardian or representative makes it for them then it is most straightforward if the child confirms that they authorise their parent, guardian or representative to make the request for them. This does not mean that the consent of a child with capacity will always be required for information about them to be given to their parent, guardian or representative, but where a formal individual rights request is received, obtaining the consent of the child will make the request more straightforward to deal with. The ICO guidance recommends this approach.

For adults without capacity, the Charity should check that anyone making requests on their behalf is authorised to do so. All individual rights requests will be handled in accordance with the law.

8. PERSONAL DATA BREACH

8.1 **Definitions**

Personal Data Breach is defined in the GDPR as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. The following is a non-exhaustive list of events which may be a personal data breach if personal data is affected:

- loss or theft of data or equipment on which personal data is stored, for example loss
- of a laptop or a paper file (this includes accidental loss);
- inappropriate access controls allowing unauthorised use of personal data;
- equipment failure;
- human error (for example sending an email or SMS to the wrong recipient);
- unforeseen circumstances such as a fire or flood; or
- hacking, phishing and other "blagging" attacks where information is obtained by
- deceiving whoever holds it.

When an event occurs, which is or may be a Personal Data Breach the following procedure will be implemented.

8.2 **Procedure for handling actual or potential personal data breaches**

Breach reporting is encouraged throughout the Charity. All individuals are expected to report any potential or actual data breaches.

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and the Charity would encourage all to report any concerns (even if they do not meet the criteria of a data breach) may have to managers or the DPL. This can help capture risks as they emerge, protect the Charity from personal data breaches and keep our processes up to date and effective.

See below for details on reporting a personal data breach

8.2.1 **Step 1: Report the Breach**

If suspecting a personal data breach, it must be reported immediately to managers or the DPL in their absence. Seek advice if unsure as to whether the breach should be reported and / or could result in a risk to the rights and freedom of individuals.

Do not wait for others to report. Duplicating reports are preferable to no reports. If the Charity's IT equipment is lost or stolen, also contact the police and get a crime reference number.

Do not try to fix or hide the breach. If a breach results from a genuine mistake, the Charity will work with individuals to learn and improve processes.

After a report is made, no further action should be taken unless instructed by the receiving manager.

8.2.2 **Step 2: Acknowledge and Document**

Upon receiving a report of a suspected personal data breach, managers must acknowledge receipt and ensure the completion of a Health & Safety reporting form available on the Teams app (Allstaff/General).

The manager will then promptly contact the DPL to together investigate and confirm whether a personal data breach has occurred. If confirmed, the following steps will be taken:

8.2.3 **Step 3: Assess and Contain**

The next step is to assess the breach by determining its extent, including what data was accessed, how many individuals are affected, and the potential impact.

The affected systems or data must be isolated immediately to prevent any further unauthorized access.

Measures must be implemented to stop the breach from continuing. Wherever possible, efforts should be made to recover, rectify, or delete any data that has been lost, damaged, or disclosed.

8.2.4 **Step 4: Assess the Risk**

The risk assessment should analyse the likelihood and severity of potential harm to the individuals affected by the breach. This includes considering the type and sensitivity of the data involved, as well as the possible consequences of the breach on those individuals.

8.2.5 **Step 5: Notify the ICO**

The ICO must be notified of a data breach within 72 hours of becoming aware of it if the breach is likely to pose a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes:

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details); or
- the exposure of the private aspect of a person's life becoming known by others. If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individual(s) must also be notified directly.

If notification to the ICO is delayed beyond 72 hours, written reasons must be documented explaining the delay. The Charity may face fines from the ICO if the breach is reported late without a valid reason.

8.2.6 **Step 6: Notify Data Subjects**

If a data breach is likely to cause a high risk to individuals' rights and freedoms, affected individuals must be informed without undue delay. The notification will include details of the breach, contact information for the DPL and the ICO, the potential consequences, and the steps the Charity has taken or plans to take to address the breach. This may involve restoring data integrity, enhancing security, and providing support to those affected.

When deciding if direct notification is necessary, managers should work closely with the DPL, the ICO, and other relevant authorities, such as the police.

If contacting individuals directly is not feasible (for example, if contact details are unavailable), the Charity should consider alternative ways to inform those affected, such as posting a statement on its website.

8.2.7 **Step 7: Notifying other authorities**

Notifying other parties should also be considered and decided on a case-by-case basis.

For example:

- Insurers;

- Parents / guardian(s) / representative(s);
- Third parties (for example when they are also affected by the breach);
- Local authority; or
- Funders/Commissioners (if required in contractual agreement)
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive

8.2.8 **Step 8: Record and Review**

All breaches must be recorded. The Charity will review the incident and response to improve policies, provide training, and implement measures to prevent future breaches.

9. COMPLAINTS FROM INDIVIDUALS

9.1 The correct procedure for raising a data protection-related complaints depends on the individual's relationship with the Charity and the nature of the issue. Individuals are encouraged to refer to the relevant policy listed below for specific guidance on how to raise a concern, how complaints will be handled, what support is available, expected response times, and rights to appeal.

Who	Procedure to Follow
Employees and volunteers acting as data subjects	Grievance Procedure
Clients, contractors, and other external data subjects	Complaints Policy
Anyone whistleblowing concerns a potential wrongdoing that could be of public interest, including unlawful processing or data breaches	Whistle blowing policy

All complaints or concerns related to data protection must be taken seriously.

9.2 Complaints to the ICO

Alternatively, you can complain directly to the Information Commissioner's Office, although the Information Commissioner's Office will usually expect you to have used the Charity's complaints process before complaining to the Information Commissioner's Office by starting a live chat or call their helpline on 0303 123 1113.

10. MONITORING AND REVIEW

10.1 This procedure is fully supported by senior management.

10.2 This procedure will be reviewed in two years unless there is a material change in responsibilities under legislation or practice

Annex 1

Department	**Contact**
Young lives	07845 642246 bridgetstratford@actionfoundation.org.uk
Language and Learning Project	*07570 623269* language@actionfoundation.org.uk
InterAction Project	07826266630 interaction@actionfoundation.org.uk
Accommodation projects	07444079678 (contactable between 9am 5pm)
Finance	finance@actionfoundation.org.uk
Business Development and Comms	comms@actionfoundation.org.uk
Others:	Data Protection Lead (DPL)– Phoebe Pham Phoebepham@actionfoundation.rg.uk info@actionfoundation.org.uk