Data Protection Policy

Introduction

Practical Action has to keep and use certain personal data about living individuals to carry out its business and meet legal obligations. The charity recognises that the lawful and correct treatment of personal data by Practical Action is important to the achievement of our objectives and to the success of our operations, and to maintaining confidence between those with whom we deal and ourselves.

The types of personal data that Practical Action may require include information about: current, past and prospective employees; Members of the charity; supporters; suppliers; and others with whom we communicate. This personal data, whether it is held on paper, on computer or other media, will be subject to the provisions of the Data Protection Act 1998.

Data Protection Principles

Practical Action fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for Practical Action must adhere to these principles.

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for those purposes;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose;
6. Be processed in accordance with the data subject's rights;
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
8. And not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Practical Action's Policy

In order to meet the requirements of the Act and its principles, Practical Action will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- take the appropriate technical and organisational security measures to safeguard personal data;
- and ensure that personal data is not transferred abroad without suitable safeguards.

Practical Action's Designated Data Controller

Practical Action and each of its subsidiaries are registered with the Information Commissioner as Data Controllers.

Practical Action's Company Secretary is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Chief Executive.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Company Secretary.

To assist in achieving compliance with the principles we have established a Data Protection Group to assist Practical Action staff in understanding and applying the data protection principles and to comply with the Act. An electronic Data Protection Guide [to be finalised] provides detailed guidance on Practical Action data protection policy and procedures.

Status of the Policy

This policy has been approved in principle by the Chief Executive and SLT. Any breach will be taken seriously and may result in disciplinary action.

Responsibility for the updating and dissemination of the policy rests with Practical Action's Company Secretary, assisted by the Data Protection Group.

Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their Line Manager or the Company Secretary in the first instance.

Subject Access

All individuals who are the subject of personal data held by Practical Action are entitled to:

- Ask what information Practical Action holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what Practical Action is doing to comply with its obligations under the 1998 Data Protection Act.

Employee Responsibilities

All employees are responsible for:

- Checking that any personal data that they provide to Practical Action is accurate and up to date.
- Informing Practical Action of any changes to information which they have provided, e.g. changes of address.
- Checking any information that Practical Action may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, employees collect information about other people (e.g. about supporters or employees of partner organisations), they must comply with this Policy and with the Data Protection Procedures (below).

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Rights to Access Information

Employees and other subjects of personal data held by Practical Action have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to Practical Action's Company Secretary.

Practical Action reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they will be amended upon request.

Practical Action aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Publication of Practical Action Information

Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on staff contained within externally circulated publications. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Company Secretary.

Subject Consent

The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate Practical Action policies, such as health and safety and equal opportunities.

Retention of Data

Practical Action will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary for operational or legal reasons.

Supporting Material

Practical Action [will] have produced a Data Protection Guide to support this policy. This document can be obtained from the Company Secretary. The purpose for holding personal data and a general description of the categories of people and organisations to whom we may disclose it are also listed in the Data Protection register. This information may be inspected or obtained from the Information Commissioner's Office.

Subject Access Policy

Practical Action will provide information in response to any reasonable subject access request. Practical Action will ensure data are kept in an accessible form to facilitate subject access.

Policy on Complaints and Queries

Practical Action will respond to any complaints as quickly and responsively as possible. Any letter we receive in relation to the Data Protection Act, that questions our policy and/or procedure will be dealt with immediately. Records will be kept of all correspondence for 5 years.

Data Protection Procedures

Recruitment

- Practical Action is clearly identified in recruitment advertisements.
- Data obtained through recruitment is not used for any other purpose.
- Staff involved in recruitment are aware of the data protection regulations and handle personal information with respect.
- Only relevant personal information is gathered.
- Information is kept secure and not disclosed to a third party.
- Information about criminal convictions is not sought unless justified by the job.
- The applicants are informed if any of the data they supply is to be checked.
- Information from applicants is kept for a period of no more than six months after the post is filled.

Staff, Volunteers, Trustees and Members

- Staff data that are kept includes (where applicable): contact details, next of kin details, bank account data for salary payment, summary information of time taken off for sickness and as annual leave.
- Accident information is kept in a Health & Safety Executive approved Accident Book.
- The computer systems used by staff are the property of Practical Action. It is made clear to staff that they should not consider email communication or file storage to be 'private'. An employee's email, file store or telephone message box may be accessed in their absence by another member of staff if necessary for Practical Action's activities and with the permission of the Director or a Programme Manager. Further information is contained in the policies on computer use.
- Personal data related to Staff, Volunteers and Trustees will be deleted within [one month] of the time they stop serving Practical Action except where it needs to be kept for statutory reasons e.g. salary records. Contact information may continue to be held if the person wishes to be kept informed of Practical Action's work.

Procedures for collecting subject data

- A Data Table [in preparation] will be kept showing all data collection points. Staff must inform the Company Secretary if they plan to access any new data from individuals.
- Staff are responsible for ensuring that data are collected accurately and fully.
- Staff are responsible for ensuring that sensitive data are identified when collected and will inform the subject that this data will be stored at the time of collection.
- All personal information should be dated at the time of collection so that records can be archived at an appropriate time.

Procedure for Data Storage and Processing

- All data processing should be included in the Data Table. Any changes to data storage or processing to be logged with the Company Secretary.

- All staff must take responsibility for following through any data care work required of them to maintain accurate organisational data systems. They are also responsible for any records they keep in any ordered filing systems.
- Archiving policies for data no longer needed in our storage systems have been set up for all data stores and must be adhered to. A clear rationale must be supplied for personal data to be kept beyond five years.
- All data will be stored in a secure location and precautions will be taken to avoid letting data become accidentally disclosed.
- Any agent employed to process data on Practical Action's behalf will be bound to comply with Practical Action's data protection policy and Data Protection legislation, by a written contract.
- Any mailings generated from stored data will observe opt out choices in good faith.
- Sensitive data will not be kept unless the Data meets criteria set by section 4(3) Schedule 3 of the Data Protection Act 1998.
- Information that is stored on a laptop must be password protected. Particular care should be taken when using a laptop in remote countries without comparable data protection legislation.

Procedure on Disclosures

- All staff must ensure any general disclosure is recorded on the Data Table and each class of disclosure includes a clear rationale as to why this is taking place.
- Any new disclosure to be made must be checked for suitability with the Company Secretary. This may be referred to the Office of the Information Commissioner (OIC) for advice.
- Any request for data based on a legal requirement, e.g. from police or other body, must be put in writing and be checked against the advice of the OIC before data are disclosed.
- All staff have a duty to protect individual's data from accidental disclosure:
    - Do not give out passwords to other people, who will then have access to the data you are entitled to view.
    - Do not recycle reports that contain personal data.
    - In particular, take due care to ensure that data is not left about on laptops or in files out of the office where they can be accessed by other people who are not Practical Action staff.
- In cases where sets of data are disclosed to non-Practical Action staff, for example data sales or swaps: staff must ensure that subjects have been informed of this use of their data, and the purpose. They must have had an opportunity to opt-out.
  Where sensitive data is involved, staff should not disclose data to outside agents unless the Data meets criteria set by Section 4(3) Schedule 3 of the Data Protection Act 1998.

Procedure on Overseas Transfer

- All staff must ensure any general overseas transfer is recorded on the Data Table and each class of transfer must include a clear rationale as to why this is taking place.
- Any new transfer to be made must be checked for suitability with the Company Secretary. This may be referred to the OIC for advice.

- Any request for data based on a legal requirement, e.g. from police or other body, must be put in writing and be checked against the advice of the OIC before data is transferred Overseas.
- Staff who take laptops overseas or who access UK data via remote access must always recognize this as a potential data transfer. Any Practical Action data must be fully protected.
- The sale or swapping of any data collected by Practical Action will only take place where the subject has been informed about this use of their data and offered the chance to opt out. Practical Action will ensure any data used in this way cannot be transferred without Practical Action's consent.
- Practical Action staff overseas who receive data from the UK must be informed that they are required to observe Practical Action's Data Protection Policy and Data Protection legislation. Where it is necessary to disclose Data in-country and where there might be conflict between National and UK privacy legislation staff should seek guidance from the Company Secretary.

Procedure on Subject Access Policy

- Staff will make every effort to ensure that immediate action is taken when a data access is requested. They will contact the Company Secretary immediately.
- A standard letter (amended as appropriate) will be sent to the subject stating Practical Action policy on subject access. This will promise to provide the required data to the best of Practical Action's ability within 40 days. Practical Action reserves the right to ask for a maximum payment of up to £10.
- A search will be set up by the Company Secretary to ensure that all relevant data will be collected and collated ready to present to the subject. The search will include all electronic data and structured manual files if required. Information on data collection, storage, processing and transfer may be required.
- The data will be offered to the subject at Practical Action's premises with a staff member on hand to help with any queries or interpretations. If the subject is unable to visit the Practical Action premises, alternative arrangements can be negotiated.

Procedure on Complaints and Queries

- Notify the Company Secretary.
- Continue to inform the Company Secretary of any correspondence and developments as they occur.