

Data Protection Policy

PURPOSE	The purpose of this policy is to ensure Banana Link complies with the law and adheres to good practice in its methods of managing data; and to protect staff and other individuals against careless and inappropriate use of private information.
SCOPE	The policy applies to all Banana Link staff (from now on, where 'staff' is used, this includes both paid staff, contracted-out consultants, volunteers and trustees).
DATE APPROVED	22 February 2011
REVIEW DATE	The first Management Committee meeting of 2014

Summary of requirements

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. The Act applies to *personal data* - information about identifiable living individuals that is held on computer or any other automated system; held in a *relevant filing system* (a paper system or a set of files that is organised alphabetically by the name of the person or some other identifier); and/or intended to go onto computer or into a relevant filing system. The core principles are:

1. Personal data should be processed fairly and lawfully.
2. Personal data should be obtained only for the purpose specified.
3. Data should be adequate, relevant and not excessive for the purposes required.
4. Accurate and kept up-to-date.
5. Data should not be kept for longer than is necessary for purpose.
6. Data processed in accordance with the rights of data subjects under this act.
7. Security: appropriate technical and organizational measures should be taken unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.

Policy statement

Banana Link is committed to complying with both the law and with good practice; and to respecting individuals' rights. This means we will only hold data with the consent of the Data Subject, or where the data is held in Banana Link's legitimate interests without infringing the Data Subject's interests. Our policy is to be open and honest with individuals whose data is held, and to provide information for staff who handle personal data to enable them to act confidently and consistently. Banana Link will notify the Information Commissioner on an annual basis about the types of information and data held, the purposes for which this data is held, and details of any transfers of information abroad.

Risks and scope

There are two key risks. Firstly, information about individuals could get into the wrong hands, through poor security or inappropriate disclosure of information. And secondly, individuals could be harmed through data being inaccurate or insufficient.

The data types included in the scope of this policy are:

- personnel records, for both staff and volunteers
- mailing list data
- donor records

The data types NOT included in the scope of this policy are (but which are subject to principles of confidentiality):

- Resources requests.
- Information about Banana Link, its plans and finances.
- Information about other organisations.
- Information which is not recorded, either on paper or electronically.
- Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a 'relevant filing system'.

Responsibilities

Banana Link is the Data Controller, and is legally and corporately responsible for complying with the Data Protection Act. Individual members of staff or volunteers are agents of the Data Controller.

Where working in close partnership with other organisations it may not be easy to identify the Data Controller, in which case guidance will be sought from the Information Commissioner.

When work is outsourced, which involves the contracting organisation having access to personal data, Banana Link will ensure that a suitable written contract is in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor.

Directors have overall responsibility for ensuring the organisation complies with its legal obligations. The responsibilities of the Data Protection Officer (Banana Link Administrator) include:

- briefing the board on Data Protection responsibilities
- reviewing Data Protection and related policies
- advising staff on Data Protection issues
- ensuring appropriate training and information about Data Protection is available
- annual notification to the Information Commissioner (which can be done online at www.ico.gov.uk)
- handling subject access requests
- approving contracts with external Data Processors (see notes)
- ensuring electronic security
- data-protection-related statements on websites and other publicity materials.

Field Officers (Solidarity Officer, Policy Analyst and International Coordinator) are responsible for being aware of the principles of Data Protection and for establishing their own procedures in accordance with

this policy. Each Field Officer must ensure the Data Protection Officer is informed of any changes in their uses of personal data. Staff are required to read, understand and accept policies and procedures that relate to the personal data they handle in the course of their work.

Subject access

Individuals have a right to know what information is being held about them. In response to a valid request, Banana Link will provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. Banana Link may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third party material where a duty of confidentiality is owed to the third party, and limited amounts of other material.

The Data Protection Officer is responsible for responding to subject access requests within the legal time limit of 40 days. Where the person managing the access procedure does not know the individual personally an identity check will be carried out before handing over any information.

Consent

There are two applicable types of consent:

- Data held on mailing lists and in personnel files (including volunteers) will only be held with the consent of the Data Subject.
- Data held on the contacts database is held in the legitimate interests of Banana Link without infringing the Data Subject's interests.

Consent may be given in writing (an application form), by email (joining an online mailing list) or verbally. Opting out from a mailing list can be effected at any time by unsubscribing or contacting the Banana Link office. Banana Link acknowledges that, once given, consent to hold data can be withdrawn, but not retrospectively.

Direct marketing and opting out

Unsolicited direct contact with individuals is treated as marketing. This includes seeking donations, marketing services and promoting events.

Banana Link will make it clear when there is an intention to use data for marketing and offer the Data Subject an opt-out tick-box at the earliest opportunity. Where lists are shared or exchanged with other organisations in order to carry out marketing-type activities, Data Subjects should be given an opt-out from their details being shared. We will only use lists from third parties where it can be guaranteed that those on the list have been given an opportunity to opt out, and where the list is deemed to be sufficiently up to date.

Staff training & acceptance of responsibilities

Staff who have access to personal data will have their responsibilities outlined during their induction procedures. Staff should also be aware of the Banana Link Secure Storage Policy. All staff will be issued with a copy of this policy and a summary will be incorporated into the Banana Link volunteers' handbook.

Policy review

The policy will be required every three years. The Data Protection Officer will initiate and lead the review, and it will be the responsibility of the Trustees to ensure it is carried out. The review should commence three months in advance of the relevant Management Committee meeting.