**TIB DATA PROTECTION POLICY (reviewed 2.12.2017)**

**POLICY INFORMATION**

Data Controller: The Data Controller is Together in Barnet

Scope of the Policy: This policy applies to

* the Trustees
* all volunteers and paid staff
* all temporary staff working on behalf of TIB

Policy Operational date: This policy comes into force on April 1st 2017

Policy Prepared by: Holly Kal-Weiss, Secretary and Trustee of TIB

Policy review date: December 1st 2018

Definitions: Unless stated to the contrary ‘Data Subjects’ in this policy includes

* Staff
* Volunteers
* Trustees
* Members
* Contractors
* Clients
* Donors
* Supporters

**INTRODUCTION**

**Purpose of the Policy**

The purpose of this policy is to enable TIB to:

* comply with the law in respect of the data it holds about individuals;
* follow good practice;
* protect TIB’s volunteers, supporters, staff, clients and other individuals
* protect the organisation from the consequences of a breach of its responsibilities
* to be compliant with GDPR rules from May 2018

**Data Protection Principles**

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Act is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall 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.

**Personal Data**

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of ‘data’ in the Act.

**Policy Statement**

TIB will:

* comply with both the law and good practice
* respect individuals’ rights
* be open and honest with individuals whose data is held
* provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

TIB recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

* keeping information securely in the right hands, and
* holding good quality information.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, TIB will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

**Key Risks**

TIB has identified the following potential key risks, which this policy is designed to address:

* Breach of confidentiality (information being given out inappropriately)
* Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
* Failure to offer choice about data use when appropriate
* Breach of security by allowing unauthorised access
* Failure to establish efficient systems of managing changes to staff and volunteers, leading to personal data being not up to date.
* Harm to individuals if personal data is not up to date
* Insufficient clarity about the way Data Subjects personal data is being used e.g. given out to general public.
* Failure to offer choices about use of contact details for Data Subjects,
* Data Processor contracts

**RESPONSIBILITIES**

**Trustees**

The Board of Trustees recognises its overall responsibility for ensuring that TIB complies with its legal obligations.

**Data Protection Lead Trustee**

The Data Protection Trustee is the TiB Secretary with the following responsibilities:

* Briefing the Board on Data Protection responsibilities
* Reviewing Data Protection and related policies
* Advising staff and volunteers on Data Protection issues
* Ensuring that Data Protection induction and training takes place
* Handling subject access requests
* Approving how data is held and processed

**Staff and Volunteers**

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

**Enforcement**

Significant breaches of this policy will be handled under TIB’s staff disciplinary procedures or the volunteers’ grievance procedure as appropriate. Members of staff breaching this policy may face dismissal.

**CONFIDENTIALITY**

**Scope**

Because confidentiality applies to a much wider range of information than Data Protection, TIB also has a separate Confidentiality Policy.

**Communication with Data Subjects**

TIB will have a privacy statement for Data Subjects, setting out how their information will be used. This will be available on request, and a version of this statement will also be used on the TIB web site. (See Appendix A.)

**Communication with Staff**

Staff, volunteers and sessional workers will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Appendix B.)

**Authorisation for disclosures not directly related to the reason why data is held**

Where anyone within TIB feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of a Data Protection Lead Trustee. All such disclosures will be documented.

**SECURITY**

**Scope**

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

**Specific Risks**

TIB has identified the following risks:

• Information could go astray or be misdirected.

• Staff or volunteers with access to personal information could misuse it.

• Staff and Volunteers could continue to be sent information after they have stopped working for TIB, if their records are not updated promptly.

• Poor web site security might give a means of access to information about individuals once individual details are made accessible on line.

• Staff may be tricked into giving away information, either about supporters or colleagues, especially over the phone, through “social engineering”.

**Setting Security Levels**

Access to information will be controlled by function.

**DATA RECORDING AND STORAGE**

**Accuracy**

TIB has several databases holding information about Data Subjects.

TIB will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

* ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
* Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
* Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
* Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
* Processing of data must be authorised by a Data Protection Lead Trustee unless it is an

established procedure previously agreed

**Retention Periods**

TIB will establish retention periods for at least the following categories of data:

* Staff
* Volunteers
* Clients
* Donors

**SUBJECT ACCESS**

**Responsibility**

Any subject access requests will be handled by a Data Protection Lead Trustee.

**Procedure for making request**

Subject access requests must be in writing. All staff and volunteers are required to pass on anything, which might be a subject access request to a Data Protection Lead Trustee without delay.

**Provision for verifying identity**

Where the individual making a subject access request is not personally known to the Data Protection Lead Trustee their identity will be verified before handing over any information

**Procedure for granting access**

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person

**TRANSPARENCY**

**Commitment**

TIB is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

* for what purpose it is being processed;
* what types of disclosure are likely; and
* how to exercise their rights in relation to the data.

**Procedure**

Data Subjects will generally be informed in the following ways:

* Staff: in the staff handbook and policies
* Volunteers: in the volunteer handbook and policies
* Sessional workers: in the staff handbook
* Supporters: when they sign up
* Clients: when they access services

Standard statements will be provided for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

**CONSENT**

**Underlying Principles**

Consent will normally not be sought for most processing of information about Data Subjects with the following exceptions:

* Staff details will only be disclosed for purposes unrelated to their work for TIB (e.g. financial references) with their consent.
* Client details will only be disclosed when permission has been obtained unless we are required to do so by law.

Information about supporters will only be made public with their consent. (This includes photographs.)

‘Sensitive’ data about supporters (including health information) will be held only with the knowledge and consent of the individual.

**STAFF TRAINING AND ACCEPTANCE OF RESPONSIBILITIES**

**Documentation**

Information for staff is contained in the staff handbook.

**Induction**

All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.

**Continuing training**

TIB will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

**NOTES**

**Data Controller**

The Data Controller is the legal ‘person’ responsible for complying with the Data Protection Act. It will almost always be the organisation, not an individual staff member or volunteer. Separate organisations (for example a charity and its trading company) are separate Data Controllers. Where organisations work in close partnership it may not be easy to identify the Data Controller. If in doubt, seek guidance from the Information Commissioner.

**Data Processor**

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

**Fair processing conditions**

Schedule 2 of the Data Protection Act lays down six conditions, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

* With consent of the Data Subject
* If it is necessary for a contract involving the Data Subject
* To meet a legal obligation
* To protect the Data Subject’s ‘vital interests’
* In connection with government or other public functions
* In the Data Controller’s ‘legitimate interests’ provided the Data Subject’s interests are not infringed

**Notification**

All Data Controllers have to consider whether they are exempt from Notification. TIB is not exempt and we have to Notify. This means completing a form for the Information Commissioner, and paying a fee. The Notification form covers:

* The purposes for which personal data is held (from a standard list) and for each purpose (again from standard lists):
* The types of Data Subject about whom data is held
* The types of information that are held
* The types of disclosure that are made
* Any transfers abroad

**Subject access**

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made.

The Data Controller 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, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. (“Third Party” means either that the data is about someone else, or someone else is the source.)

**Appendix A: Privacy statement**

When you join as a member of staff or volunteer or when you become a supporter of TIB, we obtain information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the Data Protection Act to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally the only information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system and in our databases, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

TIB may also process your data for statistical purposes but in doing this no data that will enable you to be identified will be used.

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you).

To obtain a copy, either ask for an application form to be sent to you, or write to the Data Protection Trustee at TIB. We aim to reply as promptly as we can and, in any case, meet our legal requirements.

**Appendix B: Confidentiality statement for staff and volunteers**

When working or volunteering for TIB you will often need to have access to confidential information, which may include, for example:

* Personal information about individuals who are members of staff, volunteers, clients, supporters or otherwise involved in the activities organised by TIB.
* Information about the internal business of TIB.
* Personal information about colleagues working for TIB.

TIB is committed to keeping this information confidential, in order to protect people and TIB itself. ‘Confidential’ means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by TIB to be made public.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

* not compromise or seek to evade security measures (including computer passwords);
* not gossip about confidential information, either with colleagues or people outside TIB;
* not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped volunteering or working for TIB.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality contained in the Data Protection Policy and the Confidentiality Policy of TIB.

Signed: Date:

Schedule 2:

**Conditions relevant for purposes of the first principle: processing of any personal data**

1The data subject has given his consent to the processing.

2The processing is necessary—

(a)for the performance of a contract to which the data subject is a party, or

(b)for the taking of steps at the request of the data subject with a view to entering into a contract.

3The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4The processing is necessary in order to protect the vital interests of the data subject.

5The processing is necessary—

(a)for the administration of justice,

[[F1](http://www.legislation.gov.uk/ukpga/1998/29/schedule/2#commentary-c18187811)(aa)for the exercise of any functions of either House of Parliament,]

(b)for the exercise of any functions conferred on any person by or under any enactment,

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.

SCHEDULE 3 Conditions relevant for purposes of the first principle: processing of sensitive personal data

1The data subject has given his explicit consent to the processing of the personal data.

2(1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2)The [F1 Secretary of State] may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.