CONFIDENTIALITY AND DATA PROTECTION POLICY

Purpose:	To ensure that ITF executes its duty to keep personal information safe and confidential
Version:	1
Title of originator/author:	Chief Executive / Finance Manager
Ratified by:	Board of Trustees
Date ratified:	January 2017
Frequency of review:	Every 3 years
Date of next review:	January 2020
Location of document:	SharePoint/Governance/Policies/ Confidentiality and Data Protection Policy
Links with other policies:	

CONTENTS

1. Data Protection Statement

2. Personal information will be held and used in accordance with the Data Protection Act 1998. International Tree Foundation (ITF) will not disclose such information to any unauthorised person or body but where appropriate will use such information in carrying out its various functions and services.

3. Aims and Objectives

3.1 The purpose of this Data Protection and Confidentiality Policy is to ensure that ITF executes its duty to keep personal information safe and confidential, whilst at the same time not compromising its ability to share information where it is needed.

3.2 The policy sets out the principles that must be observed by all who work within the organisation - including Trustees and volunteers - and have access to personal information.

3.3 ITF is committed to maintaining the confidentiality of personal information that it handles. Any information given or received in confidence for one purpose will not be used for another purpose, or passed to a third party, without their consent except in special circumstances e.g. to prevent harm to an individual or to prevent or detect fraud or other crime.

3.4 ITF will ensure that personal information is obtained, used and disclosed in accordance with the common law duty of confidentiality and the Data Protection Act 1998.

3.5 ITF will also have full regard for current and future legal requirements which impinge on the confidentiality of:

(a) Personal information in general, and

(b) Specific categories of personal information e.g. rehabilitation of offenders.

4. Principles

4.1 In accordance with the Principles of the Data Protection Act, personal information held in both computerised and manually filed records will:-

(a) Be obtained and processed fairly and lawfully,

(b) Be used only for the specified purposes for which it was obtained and not in any manner incompatible with those purposes,

(c) Be adequate, relevant and not excessive for those purposes,

(d) Be kept accurate and where necessary up to date,

(e) Not be kept longer than is necessary for those purposes

(f) Be processed in accordance with individuals' rights under the Data Protection Act 1998,

(g) Be protected from unauthorised access, unlawful processing, accidental loss, destruction or damage,

(h) Not be transferred to a country which does not ensure adequate protection for the rights of individuals in relation to the processing of personal information.

5. DEFINITIONS

5.1 **'Confidentiality'** applies to information whether received through formal channels (e.g. in a formal report), informally, or discovered by accident. It applies to organisational business, employees and potential employees, volunteers, clients, individuals, or organisations who come into contact with the organisation i.e. external contractors, grantees and partners.

Information which can be classified as 'Confidential', can broadly be grouped into the following areas:

(a) Information of a specific and personal nature about learner / clients, employees or volunteers

If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others.

(b) Sensitive organisational information

This may be used to damage the organisation and other organisations, as well as individuals, staff or volunteers. It may be prejudicial to the business of the organisation or used to threaten the security of its property and systems.

5.2 **'Breaches in confidentiality'** happen when sensitive information is given to people who are not authorised to access it. They are most likely to happen when procedures

have not been agreed or followed. They can also happen when information is passed between sections, departments or organisations, or when information is being stored insecurely.

6. INFORMED CONSENT

6.1 Where it is proposed, in exceptional circumstances, that information about an individual should be shared with another agency or person, the consent of the individual, or the person who provided the information, should normally be sought.

6.2 This should be done in such a way that those persons know exactly what information will be passed on, to whom and for what purpose.

6.3 Information which is confidential and restricted will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

6.4 Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information.

6.5 Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person.

6.6 Confidential information will not be discussed on the telephone unless the identity of the caller is established, this will be checked when necessary, e.g. with call-backs and/or security checks prior to the release of any information.

6.7 Refusal to give consent should be respected wherever possible.

7. EMPLOYEE RESPONSIBILITIES

7.1 In normal circumstances, staff may only disclose personal information outside the organisation if one or more of the following applies:

(a) The disclosure is routinely necessary for the purpose for which the information is held and the individuals about whom the data is held have been made aware of, or could reasonably expect, such a disclosure to be made;

(b) The disclosure is a legal requirement under the legislation governing the operation of the service or function concerned;

(c) The receiving staff member 'needs to know' the information in order to carry out their duties;

(d) The person about whom the information is held has given valid consent to the disclosure

7.2 Where it is not possible to obtain valid consent, information may exceptionally be passed on when there is a legal basis for overriding the usual non-disclosure e.g.

(a) The disclosure is required under direction of a Court Order, or in the course of law enforcement, e.g. Trading Standards co-operation with other law enforcement agencies;

(b) The disclosure is provided for agreed inter-agency procedures which have a legal basis for their operation, e.g. Area Child Protection Committee Procedures, Sex Offenders Register, Mental Health Supervision Register, Public Protection Unit and other inter-agency procedures for the assessment and management of high risk individuals;

(c) Where this is an overriding public interest in disclosing the information such as evidence of a risk of serious harm to the individual or in order to prevent or detect a serious crime.

7.3 When passing information to others, staff should:

(a) Check that the source of the request is bona fide;

(b) Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;

(c) Only send the information necessary for the purpose of the disclosure;

(d) Record exactly what has been passed on, to whom, when and why.

7.4 When receiving information from others, staff should:

(a) Ensure that any information received in confidence should be marked as such to ensure it is not inadvertently disclosed to third parties;

(b) Ensure that only information necessary for the purpose of the information being shared should be requested.

(c) Ensure that information requests include a confidentiality statement similar to "Information will be treated with utmost confidence and will not be divulged to anyone outside the organisation except when stated at collection or agreed at a later date." All confidential information shall be treated in line with ITF Confidentiality & Data Protection policy. A copy can be requested from the Data Controller.

7.5 All staff employment job descriptions and volunteer role descriptions must contain a statement enforcing the duty to respect the confidentiality of information. The employee handbook must include this obligation which then forms part of the employee's contract /volunteer's agreement.

7.6 Staff, students, staff of other agencies, temporary staff and volunteers will be asked to sign declarations of confidentiality on commencing employment with ITF either as part of their staff contract or as a separate statement.

7.7 employees and volunteers are responsible for:

(a) Checking that any personal data that they provide to ITF is accurate and up to date.

(b) Informing ITF of any changes to information which they have provided, e.g. changes of address.

7.8 Sensitive information is only to be requested on a 'need to know' basis. This means only when the information is necessary to provide a service or to manage the delivery of learning or support effectively, and then only in the best interest of service users or staff.

8. COMPLIANCE

8.1 ITF will ensure that staff, volunteers and trustees receive adequate training and guidance on their duties and responsibilities in relation to the handling, disclosure and storage of personal information.

8.2 Managers must ensure that staff and volunteers are made aware of the limits of their responsibilities, and where they may seek advice, should they have an information request which falls outside their responsibilities.

8.3 In accordance with the organisation's disciplinary procedures, disciplinary action will be taken against any member of staff who fails to carry out the duties and responsibilities set out in this Policy or the procedures which follow from it.

8.4 Where contractors and employment agencies are used, the contracts between ITF and these third parties will contain clauses to ensure that contract staff are bound by the same code of confidentiality as employed staff.

8.5 This policy has been approved by the Trustee board and any breach will be taken seriously and may result in formal action. 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 Data Controller in the first instance.

9. ITF'S DESIGNATED DATA CONTROLLER

9.1 ITF is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Chief Executive. The Data Controller is Marika Haseldine who can be contacted via e-mail: marika@internationaltreefoundation.org Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Controller.

10. DATA SECURITY

10.1 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:

(a) Any personal data which they hold is kept securely

(b) Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

10.2 Documents containing individual data must not be left visible where it can be read by anyone inappropriately. This includes telephone messages, computer prints, letters and other documents.

10.3 Desks must be cleared each evening and electronic documents closed down when leaving a desk.

10.4 All hardware containing data must be housed in a secure environment.

10.5 Personal data must not be stored on the hard disc of a laptop or data stick unless it has been encrypted. (See IT Policy)

10.6 All media containing staff information must be destroyed in a manner that ensures that data is not disclosed to an unauthorised person. Manual records should be shredded before disposal.

11. DATA PROTECTION PROCEDURES

Recruitment & Selection Collection of Information such as CV, Application Form, Personal Details	**Data Protection Rules** 1. Person should be aware that information is being collected i.e. not to be covertly obtained 2. Details collected must be kept secure 3. Only relevant details are to be collected, unless Person is informed 4. Must not ask for Criminal Convictions unless relevant to job	**Action Required** 1. All CV's, application forms etc. must be put in a password protected folder 2. All information held must be deleted when it is no longer needed
Employment Records Collection of information about employees	**Data Protection Rules** 1. Person should be aware of what information is held about them and what it is used for 2. Only relevant details, and not out of date information, are to be kept 3. Must not provide a confidential reference unless the employee knows about it 4. Employees should check their own files periodically 5. All paper files should be kept under lock and key and all computerised files should be password protected	**Action Required** 1. Ensure that everybody checked their files regularly and deletes all information that is irrelevant or out of date, and there is no business need for or legal duty to keep 3. Ensure that all relevant files are password protected by authorised personnel

	6. Any paperwork no longer need must be shredded	
Online Information Collection Collection and use of personal data online	**Data Protection Rules** 1. If using an outside company to provide services where personal information is used, a written contract must be in place to ensure security is as good as in house 2. Only collect data that is necessary at the time 3. Have an periodic audit of information collected and delete any unnecessary information 4. All information held must be secure and only authorised people must have access to the data	**Action Required** 1. Check contracts with suppliers e.g. mailing house for Data Protection policies 2.Ensure that we do not ask for bank account details etc. until needed 3. Regularly go through folders and delete any obsolete information 4. Go through folders and files and password protect, with people only having access to the files they need 5. Inform partners or organisations if information is being held on a database e.g. grant register of community organisations. 6. Confirmation required from partners about using beneficiary profiles or photographs 7. E newsletters to include an unsubscribe function

12. RIGHTS TO ACCESS INFORMATION

12.1 In accordance with individuals' rights of access under the Data Protection Act, ITF will, on request, inform an individual whether or not information is kept about them and, if so, will provide a copy of that information. Any person who wishes to exercise this right should make the request in writing to the Data Controller using the standard form which is available via the Intranet. See also Appendix I (form HR031).

12.2 ITF reserves the right to charge the maximum fee payable currently £10 for each subject access request. If personal details are inaccurate, they can be amended upon request. The only exceptions to this are current employees who are not charged for access to records held in connection with their employment.

12.3 ITF 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.

12.4 All individuals who are the subject of personal data held by ITF are entitled to:

(a) Ask what information the organisation holds about them and why.

(b) Ask how to gain access to it.

(c) Be informed how to keep it up to date.

(d) Be informed what the organisation is doing to comply with its obligations under the 1998 Data Protection Act.

13. PUBLICATION OF INTERNATIONAL TREE FOUNDATION INFORMATION

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

14. RETENTION OF DATA

14.1 ITF will keep some forms of information for longer than others depending on a number of factors e.g. funder requirements. All staff are responsible for ensuring that information is not kept for longer than necessary.

14.2 The purpose for holding personal data and a general description of the categories of people and organisations to whom we may disclose it are listed in the **Data Protection register**. This information may be inspected or obtained from the Data Controller.

APPENDIX A - DATA PROTECTION STATEMENT TO ITF MEMBERS AND DONORS

ITF is committed to safeguarding your privacy and adheres to the principles set out in the Data Protection Act 1998. Your personal details collected on this form will be used to deal with your subscription/donation; for statistical and market research purposes; to communicate (by post, telephone, SMS or e-mail) information to you about the activities of ITF.

Communications sent to you will have details of how you can unsubscribe. By completing and sending us this subscription form, you indicate your specific and informed consent to ITF's use of your personal details for the above stated purposes.

APPENDIX B - SUBJECT ACCESS INFORMATION REQUEST FORM

Under the Data Protection Act 1998, you are entitled to request access to personal information held about you by ITF. Completing this form will help to locate your information quickly and efficiently.

Section 1 – Proof of identification

In the boxes below, give details of the name of the person completing this form:

Surname:			Forename(s):	
Previous/alternative names:			Date of Birth:	
Current address:				
House/flat no & Street:			Town/City:	
County:			Postcode:	
Telephone no:			Email:	
If you are acting on behalf of the data subject please see section 2. Please state below what evidence you have enclosed (please tick):				
Birth certificate				
Passport				
Driving licence				
Two or more official letters				

Section 2 – Acting on behalf of data subject (if applicable)

If you are acting on behalf of the data subject with their written or other legal authority, please state your relationship with the data subject e.g. parent, legal guardian, or solicitor and the purpose for which the data is being collected (see notes attached)

Please enclose proof that you are legally authorised to obtain this information. The proof could be a letter of authority, letters or official forms addressed to you on behalf of the data subject. Photocopies cannot be accepted. Once entitlement has been established, we will take a copy of the documents you have supplied to us and will return the originals to you.

Please state below what proof of authority you have enclosed (please tick):

Letter of authority		Correspondence		Official Forms	

Section 3 – Data subjects details (before completion please see notes attached)

Data subject's details (if different from Section 1):

In the boxes below, give details of the name of the person of the data subject request

Additional personal information

Please provide details of any additional information i.e. previous address you feel may be of assistance to this request:

Section 4 - Declaration

Please read the following declaration carefully, then sign and date it. Please note that any attempt to mislead may result in prosecution.

I, _____(name) certify that the information provided on this application to ITF is true. I understand that it is necessary for ITF to confirm my/the data subject's identity and that it may be necessary for ITF to request more details from me in order to be able to locate the correct information.

Print Name: _____ Date: _____

Signature:

_____

OFFICIAL USE ONLY:

Date received:		Identity confirmed:	
Enquiry Log No:		Date responded:	

NOTES:

Consent to application by a Third Party: Under the Data Protection Act 1998, an individual is entitled to ask ITF for a copy of personal information which it holds about him/her for the purposes of providing services to the individual. The information, which the individual is entitled to receive from ITF includes a description of these purposes, recipients to whom the data are disclosed and the sources of the data. This entitlement is known as the 'Right of Access to Personal Data'. This access may also be granted by another person acting on behalf of the data subject providing written consent is given by the data subject.

Please note that in general requests for information about a person other than yourself will be rejected except in the following situations:

Parents can request information about their children if they are under 16 years of age although there is not automatic right to the data

A solicitor may request information on behalf of a client