



# General Data Protection Regulation Policy

This policy will be reviewed on an ongoing basis, at least once a year. Time to Help UK will amend this policy, following consultation, where appropriate.

Date of last review: 11/03/2022



# Contents

1	Introduction.....	4
2	Data Protection Policy .....	4
	POLICY STATEMENT .....	4
	LEGAL REQUIREMENTS .....	4
	MANAGING DATA PROTECTION .....	4
	PURPOSE OF DATA HELD BY THE COMMUNITY ASSOCIATION.....	5
	DATA PROTECTION PRINCIPLES .....	5
2.1	Fairly and lawfully processed personal data.....	5
2.2	Processed for limited purpose.....	5
2.3	Adequate, relevant and not excessive.....	6
2.4	Accurate and up-to-date.....	6
2.5	Not kept longer than necessary.....	6
2.6	Processed in accordance with the individual’s rights .....	6
2.7	Secure Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.....	6
2.8	Not transferred to countries outside the European Economic Area, unless the country has adequate protection for the individual. ....	7
3	Gdpr applies to:.....	7
	Personal data .....	7
	Automated Personal Data and Filing Systems .....	7
	Sensitive personal data .....	7
	Awareness .....	7
	Accountability.....	7
	Information we hold .....	8
	Data Protection by Design and Data Protection Impact Assessments .....	8
4	Data Processor .....	8
5	Consent.....	9
	Definition.....	9
	Giving Consent .....	9
6	Other Legitimate Interests.....	10
7	Communicating privacy information .....	10
8	Annexes.....	11



8.1 Annex A..... 11

8.2 Annex B ..... 12

9 Website Statement. .... 14

10 Time to Help UK's Privacy Statement..... 15

11 Consent..... 17



## 1 INTRODUCTION.

---

This document highlights the key themes of the Data Protection Policy and General Data Protection Regulation (GDPR) to help us understand the new legal framework in the EU. It explains the similarities with the existing UK Data Protection Act 1998 (DPA), and describes some of the new and different requirements. It is aimed at those who have day-to-day responsibility for data protection. The GDPR applied in the UK from 25 May 2018.

Application. The GDPR applies to 'controllers' and 'processors' who have new obligations under the GDPR. The definitions are broadly the same as under the DPA and we can assume that we will be subject to the GDPR. Time To Help UK will have significantly more legal liability if we are responsible for a breach. The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

## 2 DATA PROTECTION POLICY

---

### POLICY STATEMENT

Time to help UK is committed to a policy of protecting the rights and privacy of individuals, voluntary and community group members, volunteers' staff and others in accordance with The Data Protection Act 1998. The policy applies to all voluntary and community group members and staff at the community Centre. Any breach of The Data Protection Act 1998 or The Community Centre Data Protection Policy is considered to be an offence, and, in that event, disciplinary procedures apply.

As a matter of good practice, other organisations and individuals working with the Centre, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to abide by this policy.

### LEGAL REQUIREMENTS

Data are protected by the Data Protection Act 1998, which came into effect on 1 March 2000. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data are not processed without their knowledge, and, wherever possible, is processed without their consent.

The Act requires us to register the fact that we hold personal data and to acknowledge the right of 'subject access' – voluntary and community group members and staff must have the right to copies of their own data.

### MANAGING DATA PROTECTION

We will ensure that our details are registered with the Information Commissioner.

## **PURPOSE OF DATA HELD BY THE COMMUNITY ASSOCIATION**

Data may be held by us for the following purposes:

1. Staff Administration
2. Fundraising
3. Realising the Objectives of a Charitable Organisation or Voluntary Body
4. Accounts & Records
5. Advertising, Marketing & Public Relations
6. Information and Databank Administration
7. Journalism and Media
8. Processing for Not for Profit Organisations
9. Research
10. Volunteers

## **DATA PROTECTION PRINCIPLES**

In terms of the Data Protection Act 1998, we are the 'data controller', and as such determine the purpose for which, and the way, any personal data are, or are to be, processed. We must ensure that we have:

### **2.1 FAIRLY AND LAWFULLY PROCESSED PERSONAL DATA**

We will always put our logo on all paperwork, stating their intentions on processing the data and state if, and to whom, we intend to give the personal data. Also provide an indication of the duration the data will be kept.

### **2.2 PROCESSED FOR LIMITED PURPOSE**

We will not use data for a purpose other than those agreed by data subjects (voluntary and community group members, staff and others). If the data held by us are requested by external organisations for any reason, this will only be passed if data subjects (voluntary and community group members, staff and others) agree. Also, external organisations must state the purpose of processing, agree not to copy the data for further use and sign a contract agreeing to abide by The Data Protection Act 1998 and (your name here) Data Protection Policy.



### 2.3 ADEQUATE, RELEVANT AND NOT EXCESSIVE

The Association will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

### 2.4 ACCURATE AND UP TO DATE

We will provide our members (voluntary and community group members, staff and others) with a copy of their data once a year for information and updating where relevant. All amendments will be made immediately, and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data held by us are accurate and up to date. Completion of an appropriate form (provided by us) will be taken as an indication that the data contained are accurate. Individuals should notify us of any changes, to enable personnel records to be updated accordingly. It is the responsibility of the Association to act upon notification of changes to data, amending them where relevant.

### 2.5 NOT KEPT LONGER THAN NECESSARY

We discourage the retention of data for longer than it is required. All personal data will be deleted or destroyed by us after one year of non-membership has elapsed.

### 2.6 PROCESSED IN ACCORDANCE WITH THE INDIVIDUAL'S RIGHTS

All individuals that the Association hold data on have the right to:

- Be informed upon the request of all the information held about them within 40 days.
- Prevent the processing of their data for the purpose of direct marketing.
- Compensation if they can show that they have been caused damage by any contravention of the Act.
- The removal and correction of any inaccurate data about them.

### 2.7 SECURE

**APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES SHALL BE TAKEN AGAINST UNAUTHORISED OR UNLAWFUL PROCESSING OF PERSONAL DATA AND AGAINST ACCIDENTAL LOSS OR DESTRUCTION OF DATA.**

All Association computers have a log in system and our Contact Database is password protected, which allow only authorised staff to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in a locked filing cabinet and can only be accessed by the Executive officers. When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

## 2.8 NOT TRANSFERRED TO COUNTRIES OUTSIDE THE EUROPEAN ECONOMIC AREA, UNLESS THE COUNTRY HAS ADEQUATE PROTECTION FOR THE INDIVIDUAL.

Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual. The Association takes particular care to be aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the European Economic Area.

### 3 GDPR APPLIES TO:

---

**PERSONAL DATA.** Like DPA, GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. Keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference.

**AUTOMATED PERSONAL DATA AND FILING SYSTEMS.** GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

**SENSITIVE PERSONAL DATA.** GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

**AWARENESS.** The decision makers and key people in our charity were made aware that the law is changing to the GDPR, in a briefing, and appreciate the impact this is likely to have. TIME TO HELP UK has looked at areas that could cause compliance problems identified under GDPR and has not discovered any issues. If issues arise in the future, they will be recorded on the risk register, where there is a place holder. TIME TO HELP UK is raising awareness, across the organisation of the changes that are coming.

**ACCOUNTABILITY.** TIME TO HELP UK has set comprehensive but proportionate governance measures, management support and direction for data protection compliance in a framework of policies and procedures. Our charity monitors compliance with data protection policies and regularly reviews the effectiveness of data handling / processing activities and security controls. Our charity has developed and implemented a needs-based data protection training programme for all staff. Appropriate technical and organisational measures that ensure and demonstrate that we comply are in place: data protection policies, staff training and internal audits of processing activities and reviews of internal HR policies.

**INFORMATION WE HOLD.** Our charity has documented what personal data we hold, where that data came from and who it is shared with. We will never share any personal data with any third parties other than government officials (e.g. HMRC, Police)

**DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS.** Our charity has implemented appropriate technical and organisational measures which show we have considered and integrated data protection into your processing activities.

## 4 Data Processor

---

As much of the processing is wholly or partly performed by a data processor: that processor will always assist in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances.

**Data Protection Officers.** Time to Help UK has designated responsibility for data protection compliance to a suitable individual within the organisation. The COO has been appointed as Data Protection Officer (DPO). It should be noted that Time to Help UK does not carry out large scale monitoring of individuals or large-scale processing of special categories of data or data relating to criminal convictions and offences.

Lawful basis for processing personal data. Our charity has reviewed the various types of processing we carry out. We have identified our lawful basis for your processing activities and documented this, and:

Time to Help UK has explained our lawful basis for processing personal data in our privacy notice(s). In a data sharing context, our privacy notice tells the individual:

- Who we are?
- Why we are going to share personal data.
- Who we are going to share it with?
- We provide a privacy notice when we first collect a person's personal data.
- If we have already collected their personal data, then we provide them with the information above as soon as we decide that we are going to share their data or as soon as possible afterwards.

Article 6(1) of the GDPR sets out the conditions that must be met for the processing of personal data to be lawful. The conditions, which Time to Help UK adheres to, are:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject;



- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. These conditions are all equally valid and Time to Help UK Assesses which of these grounds are most appropriate for different processing activities and then fulfil any further requirements the GDPR sets out for these conditions (GDPR Article 5). Processing activities that fall under performance of a contract, legal obligation, vital interests and public task may be fairly straight-forward to identify. The key is assessing whether Consent or Legitimate Interests will be most appropriate for specific processing of personal information

## 5 CONSENT

---

As a legal ground for processing personal data.

**DEFINITION.** GDPR defines Consent in Article 4(11) as: ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It should be noted that our charity does not offer services directly to children.

**GIVING CONSENT.** Our charity has reviewed how we seek, record and manage consent. and the systems currently used to record consent and implemented appropriate mechanisms in order to ensure an effective audit trail. Consent requires a positive opt-in and should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting the website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. It should be noted that Time to Help UK: **Does not use pre-ticked boxes or any other method of consent by default.**

Requires consent to be named, i.e. third parties with whom the data may be shared will, with the exception of: nominated welfare referees (given by the beneficiary), other service charities (given by the beneficiary) donors who have been specified, IT support (if

requested) and travel agents dealing with transport (requested) , will where possible be specifically named. Simply providing categories of third parties will not be acceptable. Aims to ensure consent is granular, i.e. separate consent is obtained for independent processing operations. Ensures consent isn't a pre-condition to receive our services but for website registration agreement with our data protection policy is required. It does not bundle it in with Terms & Conditions. Ensures consent is only be relied upon if; there is no other lawful basis for processing; we can give individuals a genuine choice or when we are required to have consent i.e.: for electronic marketing.

## **6 OTHER LEGITIMATE INTERESTS**

---

There are other legitimate interests as a legal ground for processing personal information. The ICO has set up a Working Party, to produce guidance for commercial and not-for-profit organisations on the use of Legitimate Interests under the General Data Protection Regulation (GDPR). The ICO's draft guidance on Consent states: 'consent is one lawful basis for processing, but there are five others. Consent won't always be the easiest or most appropriate'. When considering whether you can rely on Legitimate Interests, Time to Help UK uses four key factors:

It will be necessary to demonstrate that Time to Help UK has balanced its interests with the interests and rights of the individuals affected by your proposed processing activity.

The assessment, which may be a simple process or very detailed in more complex scenarios, will be documented as it may be challenged by individuals or the Regulator.

Time to Help UK will inform individuals that we are processing their personal information under this condition (i.e. via our Privacy Policy). Time to Help UK will need to be able to uphold the individual's right to object to such processing.

Recital 47 of the GDPR broadly describes areas where Legitimate Interest might be relied upon, for example when the processing is strictly necessary for the purposes of preventing fraud or ensuring network security, where there is a 'reasonable expectation' or a 'relevant and appropriate relationship'. Recital 47 also specifically mentions; 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate purpose'.

## **7 COMMUNICATING PRIVACY INFORMATION**

---

Our charity has reviewed our current privacy notices and has a plan in place to make any necessary changes in time for GDPR implementation, including the need to explain the legal basis for holding information.

Individuals' rights. Our charity has checked your procedures to ensure that you can deliver the rights of individuals under the GDPR.

Subject access. Our charity has reviewed our procedures and has plans in place for how we will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR.

Breach notification. Time to Help UK has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. Our charity has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage e.g. through identity theft or confidentiality breach. This includes a mechanism to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

Transfer of data. Our charity operates in more than one EU member state but the UK ICO is the lead supervisory authority.

## **8 ANNEXES**

---

- Process for Data Protection Impact Assessments.
- Data protection, privacy and communications policy

### **8.1 ANNEX A.**

Process for Data Protection Impact Assessments.

Our charity understands when we must conduct a data protection impact assessment (DPIA): a tool which can help identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. We have carried out an initial DPIA and because the type of processing we do is not likely to result in a high risk to the rights and freedoms of individuals, we do not currently believe we have a problem. We will, however, undertake a DPIA in cases where it is unclear whether doing so is required. It will contain the following information:

- A description of the processing operations and the purposes including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals. The measures in place to address risk, including security and to demonstrate that you comply.

A DPIA can address multiple processing operations that are similar in terms of the risks presented, providing adequate consideration is given to the specific nature, scope, context and purposes of the processing. If the processing is wholly or partly performed by a data

processor, then that processor will assist in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances.

## 8.2 ANNEX B

Data protection, privacy and communications policy.

**Introduction.** The Charity holds personal data about job applicants, employees, beneficiaries, partners, donors and other individuals for a variety of purposes connected with the Charity's work. This policy sets out how the Charity seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Managing Director should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

**Scope.** This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers. All staff must be familiar with this policy and comply with its terms. The Charity may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Definitions. In this policy:

Business purposes means the purposes for which personal data may be used by the Charity, e.g. personnel, administrative, financial, regulatory, payroll and fund-raising purposes;

Personal Data means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, interns, volunteers, beneficiaries, partners and donors. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual.

**Sensitive Personal Data.** Means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy

**Processing Data.** Means obtaining, recording, holding or doing anything with it, such as organising, using, altering, retrieving, disclosing or deleting it

**General principles.** The Charity's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All employees have personal responsibility for the practical application of the Charity's data protection policy. The Charity will observe the following principles in respect of the processing of personal data:

- to process personal data fairly and lawfully in line with individuals' rights;
- to make sure that any personal data processed for a specific purpose are adequate, relevant and not excessive for that purpose;

- to keep personal data accurate and up to date;
- to keep personal data for no longer than is necessary;
- to keep personal data secure against loss or misuse;
- not to transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without adequate protection.
- Fair and lawful processing. Staff should generally not process personal data unless:
  - the individual whose details are being processed has consented to this;
  - the processing is necessary to perform the Charity's legal obligations or exercise legal rights;
  - the processing is otherwise in the Charity's legitimate interests and does not unduly prejudice the individual's privacy;

**Gathering Data.** When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the COO.

**Sensitive Data.** It will normally be necessary to have an individual's explicit consent to process 'sensitive personal data', unless exceptional circumstances apply, or the processing is necessary to comply with a legal requirement. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the Managing Director for more information on obtaining consent to process sensitive personal data.

**Accuracy, adequacy, relevance and proportionality.** Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the Charity to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the COO.

Staff must ensure that personal data held by the Charity relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the Charity so the Charity's records can be updated.

**Security.** Staff must keep personal data secure against loss or misuse. Where the Charity uses external organisations to process personal data on its behalf additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the Managing Director to discuss the

necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

Data retention. Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data were obtained.

Rights of individuals. Individuals are entitled (subject to certain exceptions) to request access to information held about them. All such requests should be referred immediately to the COO. This is particularly important because the Charity must respond to a valid request within the legally prescribed time limits.

Reporting breaches. Staff have an obligation to report actual or potential data protection compliance failures to the Managing Director. This allows the Charity to:

- Investigate the failure and take remedial steps if necessary.
- Make any applicable notifications.

Consequences of failing to comply. The Charity takes compliance with this policy very seriously. Failure to comply puts both staff and the Charity at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

## **Non-adherence**

Breaches of this policy will be dealt with under the Grievance and/or Disciplinary procedures as appropriate.

## **Legislative Framework**

The Organisation will monitor this policy to ensure it meets statutory and legal requirements including the Data Protection Act, Children's Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act. Training on the policy will include these aspects.

## **Ensuring the Effectiveness of the Policy**

All Executive Committee members will receive a copy of the confidentiality policy. Existing and new workers will be introduced to the confidentiality policy via induction and training. The policy will be reviewed annually, and amendments will be proposed and agreed by the Executive Committee.

## **9 WEBSITE STATEMENT.**

---

Time to Help UK is committed to protecting individuals' privacy. This policy describes how Time to Help UK collects and uses personal information about people who visit our websites

and give us their data over the phone, face to face, and in writing. The terms of this policy may change, so please check it from time to time. If you have any queries about this policy please contact:

Time to Help UK, 337 Fore Street, London, N9 0NU or mail to [legal@timetohelp.org.uk](mailto:legal@timetohelp.org.uk)

**How do we collect information?** We may collect personal information from a variety of sources, including from individuals, their organisation or their partners. We may collect personal information when individuals register with us as a user of the portal, complete a beneficiary or donor application or report, participate in our events or when individuals communicate with us by e-mail, telephone or in writing.

**What information do we collect?** In general, the personal information we collect includes (but is not limited to): name, contact details (including phone numbers and electronic and postal addresses), and organisational and employment details where an individual is a member of staff or trustee or otherwise linked to an organisation. We also collect information that is not personal information. For example, we may collect information relating to an individual's deployments, passport details, next of Kin. We generally use this information in order to be able to contact individuals and to analyse trends across the programme; to report statistics and data; who is involved and how. We also use this information to support us to deliver the programme, diagnose problems; target and improve the quality of the programme for the areas and residents it aims to support.

**How do we use this information?** We will use an individual's personal information for:

- Dealing with enquiries and requests;
- Checking the eligibility of beneficiaries;
- Checking the credentials of donors;
- Providing information about products and services;
- For administrative purposes;

## **10 Time to Help UK's Privacy Statement.**

---

The Data Protection Act 1998 and GDPR provide the legal framework that defines how personal information can be used. TTH UK is fully committed to complying with the Data Protection Act 1998 and has a legal duty to protect any information we collect. Personal information is only used for the purpose for which we collect it. Only information that we actually need is collected. Relevant Personal information is only seen by those who need it to do their jobs, for example passport details to travel agents, special requirements, to accommodation donors.

We will not pass an individual's personal information on to any other organisation without the individual's consent unless we are required to do so by law. Personal information is retained only for as long as it is required for the purpose collected. We will, where necessary, keep individuals' personal information up to date. Personal information will be protected from unauthorized or accidental disclosure. We will provide individuals with a copy of their

personal information on request. Inaccurate or misleading data will be corrected as soon as possible.

These principles apply whether we hold individuals' personal information on paper or in electronic form.

**Access Rights and Requests.** The data subject has the right to see what personal data we hold about them. Subject access requests must be submitted in writing. Should the data subject wish to obtain a copy of the personal information we hold about them, a request should be submitted to: Time to Help UK, 337 Fore Street, London, N9 0NU or mail to [legal@timetohelp.org.uk](mailto:legal@timetohelp.org.uk)

How do we protect personal information? Other than in relation to Non-Confidential Information, we will take all reasonable steps to protect the personal information that we hold from misuse, loss, or unauthorised access, including by means of firewalls, password access, secure servers and encryption of financial transactions. We take appropriate measures to ensure that the personal information disclosed to us is kept secure, accurate, and up to date. We will ensure that individuals' personal information is kept only for so long as is necessary for the purposes for which it was collected and is securely destroyed in accordance with our data retention and disposal policy.

Will we disclose the information we collect to outside parties? We will only disclose data when obliged to disclose personal data by law, or the disclosure is 'necessary' for purposes of national security, taxation and criminal investigation, or we have the individual's consent, and to the following:

Other entities that Time to Help UK works with including our donors, other service charities and sponsors where specific information is required, and it is in the interest of the beneficiary to do so.

Suppliers we engage to process data on our behalf. In such cases information is only shared for the purpose of providing services on our behalf relating to communications, or agreements between the individual and Time to Help UK. Such processing is conducted under relevant Data Processing Agreements.

We will not sell any information relating to individuals' web browsing activity.

Trademarks and copyright. Time to Help UK's website contains material which is protected by copyright and/or other intellectual property rights. All copyright and intellectual property rights including the names, images and logos are owned by Time to Help UK unless otherwise stated. All rights are reserved. Users are responsible for complying with all applicable copyright laws. We permit individuals to make copies of information on TRBL Group websites as necessary incidental acts during their viewing and a printed copy may be taken for personal use of so much of the site as is reasonable for private purposes. All other uses are prohibited. Nothing in these terms shall be construed as conferring any right to use any trademark logo patent right or copyright of Time to Help UK.



## 11 CONSENT

---

By providing us with personal information, users confirm that consent is given and or has been obtained for the collection and use of this in accordance with the purposes described in this policy.

### Changes

If the personal details provided change, please help us to keep the information provided to us up to date by notifying [enquiries@giveustime.org.uk](mailto:enquiries@giveustime.org.uk)

### Data Protection Regulator

Further information and advice about data protection is available from: The Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel: +44 (0) 01625 545 745. Website: [www.ico.org.uk](http://www.ico.org.uk)

---

End of Policy

