Timebanking UK - Data Protection, Privacy and Information Security Policy

This privacy policy sets out how Timebanking UK (TBUK) uses and protects any information that you give TBUK when you use our website or software platforms. Timebanking UK is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified, you can be assured that it will only be used in accordance with this Policy.

Personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the latest versions of relevant official regulations like GDPR (see Legislation section below).

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our Organisation treats personal information lawfully and correctly.

For the purposes of the new General Data Protection Regulation 2018, TBUK is a Data Processor in its relationship with time banks, and the Data Controller when working on its own activities. Please note that TBUK is able to access data for any member who has joined a time bank that uses TBUK's software. The information you provide will be held in accordance with the GDPR and may be used by TBUK and its member time banks. Member time banks have signed up for TBUK membership and are using the software provided by TBUK for recording information about their members and time exchange activities.

Note that Timebanking UK may be a distinct entity from your local time bank, and you should consult your time bank coordinator for policy as it pertains to membership with them separate to Timebanking UK, Time Online 2, www.timebanking.org and any other Timebanking UK system or platform.

What we collect

Timebanking UK collect organisational information for the use of creating and supporting time banks. This may involve sending out updates and information to do with timebanking in general as well as items specific to an individual time bank, and we may also use Email addresses for the express purpose of sending out a newsletter or important information, such as policy updates. Although Timebanking UK will not directly collect any data from people who join a time bank for its own purposes, the time banks themselves may collect the following information:

- name and date of birth
- contact information including email address, and postal address
- Some sensitive information may be requested, namely ethnicity, gender and medical history If any other sensitive information is required, the time bank will inform their members directly
- demographic information such as postcode, preferences and interests
- other information relevant to the running of specific time banks

What we do with the information we gather

Our time banks require this information both as a record system of membership and the time transactions that you have been part of, and in order to understand their members' needs and provide a reactive and supportive service, and particularly for the following reasons:

- internal record keeping
- TBUK, and the time banks, may use the information to improve our products and services
- TBUK may use anonymised data for statistical reporting and analysis purposes, including, but not limited to, numbers of time bank members using the system, and how many hours have been exchanged – as displayed on the home page of Timebanking UK for example
- TBUK may use anonymised data for statistical reporting in partnership with contracted associates or not-for-profit organisations with the sole purpose of improving the service.
- we may directly contact members in certain circumstances during the time they are part of the system, if we deem there is an emergency or there is an issue with the data retention.
- We may also contact members directly if there is a change to this policy, including via newsletter or by contacting your local time bank co-ordinator as appropriate

Who will we share this with?

Sometimes time banks need to share your information with other members. They will only do this when it is necessary in order to offer you this service, or if required to do so by law. Any contracted associate or not-for-profit 3rd party TBUK engages to improve the service provided by TBUK will be strictly vetted and cyber essentials compliant where necessary, and supplied with fully anonymised data under full oversight of TBUK and in accordance with all statutory requirements of GDPR.

Where we store your personal data

The data that we collect from you will be stored in the European Economic Area ("EEA"), It will be processed by members of Timebanking UK, the developers of the software you use to manage your timebanking and in exceptional circumstances by staff at the database hosting company to allow for repair to damaged systems or hardware upgrade, for example. This means that it may, potentially be processed by staff operating outside the EEA who work for suppliers. In such cases, we rely on the vetting process of our trusted partners.

By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this policy and with GDPR.

All information you provide to us is stored on secure servers. Where we or our time banks have given you (or where you have chosen) a password which enables you to access certain parts of our website, systems or other software, you are responsible for keeping this password confidential. We ask you not to share a password with anyone. Where possible, please ensure your devices have up to date malware protection, up to date web browsers and any software is updated to the most recent version. We also recommend that any device capable of such has multi factor authorisation enabled and uses strong passwords that are not shared with anyone, as appropriate.

Unfortunately, the transmission of information via the internet is never completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to prevent unauthorised access. If any breach in data is detected, we will contact you, or your timebank co-ordinator as appropriate

How long will we keep it for?

We will only keep this information for as long as necessary or as the law requires. For the purposes of this service, we will keep this information whilst a member is a part of the scheme and for a period of no more than 24 months after. If you wish to leave the scheme, you can do this at any time by contacting your local time bank co-ordinator.

What if something changes?

If the information you provided or your circumstances change, please contact your local timebank co-ordinator. If there are changes to this policy outside of the Date for Review (see end of document), we will contact you or your local time bank co-ordinator, and/or in newsletter or other update to you or your local time bank co-ordinator.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we, and our hosting company, have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online, including but not limited to strict organisational protocols, adherence to GDPR and government backed Cyber Essentials accreditation for certified cyber security.

Controlling your personal information

We will never sell, distribute or lease your identifiable personal information to third parties unless we have your Permission, instruction or are required by law to do so. TBUK or your local time bank may use the organisations anonymised data to improve services, for example, by reporting the amount of help given in a particular area or in support of a particular cause. Our time banks may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen. You may request details of personal information which we hold about you under the General Data Protection Regulation. A small fee of up to £10 may be payable. If you believe that any information we are holding about you is incorrect or incomplete, please write to or email us as soon as possible. We will promptly correct any information found to be incorrect.

Your rights

Every person has the right to request copies of the personal information an organisation holds about them and the reason the data was used. This is called a subject access request (SAR). The law also provides you with other rights regarding your information including for example; correction of inaccurate data, objection to processing, moving your information to somewhere else, and in some cases, getting your information deleted. If you are unhappy with the way your data is being handled or if you need to correct or update any data, please contact your local time bank co-ordinator. You may also contact Timebanking UK. Note that there is a minimum amount of data required for Timebanking to function. If you are not satisfied with any response you may receive from us based on a complaint or concern about your personal information, you then have the option of contacting the Information Commissioners Office to take that complaint further. The Information Commissioners Office does like to see that you have raised a complaint with an agent first and received a response before contacting them. If you do wish to contact them, the address details can be found below:

The Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF

Telephone: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

Website: www.ico.org.uk

Email: casework@ico.org.uk

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Access to information

GDPR gives you the right to access information held about you. Your right of access can be exercised in accordance with the Act. Any Subject Access Request may be subject to a fee of £10 to meet our costs in providing you with details of the information we hold about you.

Timebanking UK will respond positively to access requests, replying as quickly as possible, and in any event within the 40-day time limit. Whilst individuals have a general right of access to any of their own personal information which is held, the Organisation will be mindful of those circumstances where an exemption may apply. See www.ico.org.uk for further details.

The Organisation will only disclose personal data to those recipients listed in the Notification Register, or whenever it is otherwise permitted by law to do so. The Organisation will always endeavour to seek the permission of the data subject where it is required by law to do so.

Legislation

Most businesses hold personal data on their customers, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation on a national and European level.

These include:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
- Data Protection Act 1998
- Computer Misuse Act 1990.

Timebanking UK will, through appropriate management, strict application of criteria and controls ensure that it:

- observes fully the conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information, and only to the extent that it is needed to fulfil
- operational needs or to comply with any legal requirements
- ensure the quality of information used
- apply strict checks to determine the length of time information is held
- ensure that the rights of people about whom information is held, can be fully exercised under the Act (these include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal

- information
- not use information for a purpose which is incompatible with the original purpose for which
- permission was given by the data subject
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- allocate such resources as may be required to ensure the effective operation of the Policy.

In addition, Timebanking UK ensures that:

- there is someone with specific responsibility for Data Protection within the Organisation: The signee of this policy is the manager for data protection within Timebanking UK.

It is the remit of the data protection manager to ensure that all policies are known and understood, adhered to at all times, are available to all staff and that these policies are kept up to date to ensure that:

- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised
- anybody wanting to make enquiries about handling personal information knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are clearly described
- a regular review and audit are made of the way personal information is held, managed and used
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- a breach of the rules and procedures identified in this Policy will be dealt with using our most severe disciplinary processes including suspension or dismissal.

The General Data Protection Regulation principles

GDPR applies to every organisation that handles (processes) personal information such as names (data) on living individuals (subjects). The Act has seven data protection principles, which are intended to guide the interpretation and implementation of the Act. These principles are, personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

7. “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

Computer misuse

Timebanking UK strictly adheres to and enforces the Computer Misuse Act 1990, which makes it an offence to gain unauthorised access to a computer, even if no damage is done and no files are deleted or changed. Anyone who accesses a computer without authorisation, say by guessing a password, faces a maximum six-month prison sentence, or a maximum fine of £2,000, or both.

If an individual gains unauthorised access with the intent to commit a further offence, for example access your bank account online to transfer money, they face five years’ imprisonment and/or a fine. This Act also makes it an offence to purposefully change files on a computer with intent and without

authorisation. This could include deleting files or even changing computer settings. Anyone who does so, even if there is no intent to defraud or do damage, faces a maximum prison sentence of five years and/or an unlimited fine.

Controlling access

Timebanking UK controls access to stored data by restricting access to employees needing specific data in order to carry out their jobs. The Organisation takes steps to prevent accidental loss or theft of personal data by using server backup processes and ensuring that all data is stored remotely and guarded by secure firewalls.

- Four administrators have access to our platform who work for Timebanking UK and Bankside Systems (the developers of our online platform, Time Online 2)
- We have strong, current password protection policy, and all passwords are resistant to brute force attacks as per governmental Cyber Essentials protocol.
- Our employee's personal and company supplied access devices have up to date firewalls and anti-malware software.
- Should there be any non-compliance with any cyber security policy then staff will be subject to retraining, followed by disciplinary procedures up to and including suspension, dismissal and legal action where appropriate.
- Timebanking UK employees, associates and partner organisations are subject to pre-employment screening and references, along with Google checks and social media checks, and are expected to be in compliance with national or international regulations where appropriate.

Physical and environmental security

Timebanking UK is entirely remote and cloud based as of 21/07/23 and will remain so on a permanent basis.

- All company property used for the purposes of executing employee duties are registered, secure, have up to date software and hardware, and all password or protective protocols are in place, including multifactor authentication where applicable.
- All company data is cloud based and no new hard copies are used or stored.
- Any hard copies made prior to this are securely stored and only held as per statutory requirements and then destroyed.

Outsourced risks

Our outsourced risk is our platform developers who have a disaster recovery system which is the entire website and its database, which are backed up each night, compressed, encrypted and then uploaded to one of their servers outside of the data centre network. So, in the event of a catastrophic failure at the datacentre they would be able to get the platform up and running again on another server within a business day.

Responsibilities & review

The Board of Trustees have overall responsibility for the administration and implementation of the organisation's Data Protection Policy, with the primary point of contact being the signee of this document. This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to GDPR or whenever deemed necessary.

The Data Protection Policy will, under normal circumstances, be managed and reviewed annually. The reviews to the Policy will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the Policy will be reviewed sooner in the event of any one or more of the following:

- Weakness in the Policy is highlighted
- Weaknesses in hardware and software controls are identified
- In case of new threat(s) or changed risks
- Changes in legislative requirements
- Changes in Government, company or other directives and requirements.

Document management

Signed:  Name: Sarah Bird

Position: CEO Date 21/07/2023

Contact: Info@timebanking.org

Board approval: 21/07/2023

Date for next review: 21/07/2024

Timebanking UK