PRIVACY POLICY

BACKGROUND

WHAT IS GDPR?

The General Data Protection Regulation (GDPR) is designed to replace and modernise the current Data Protection Act. Building on the principles already in place, it aims to give individuals more control over their personal information (PI) and make organisations more accountable for how they use and protect PI.

WHO DOES GDPR APPLY TO?

Any organisation that collects, uses, shares personal information about individuals will be obliged to meet GDPR requirements. That includes the personal information of our customers, employees and any other individuals that we collect or store information about. Everyone at TLCCH has a responsibility to ensure we are meeting this regulation.

WHEN DID THE GDPR COME INTO EFFECT?

GDPR came into effect on the 25th May 2018 replacing the current DPA with significant changes to current data protection laws as we know them. If we are not aligned with the regulation, we could face hefty fines, for the loss, misuse, inaccuracy of personal information or for failing to meet individual rights.

WHAT ARE THE PENALTIES BE FOR FAILING TO COMPLY WITH GDPR?

The maximum fine a company can face is 4% of their annual global turnover, or €20 million, whichever is the highest.

WHAT KIND OF INFORMATION DOES THE GDPR APPLY TO?

Much like the Data Protection Act 1998, GDPR applies to personal information including special category (sensitive personal information e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation). Criminal convictions and offences are no longer classed as special category personal information but similar extra safeguards must still be applied.

Personal information can be any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites or a computer IP address.

IT DOES NOT APPLY TO ANY DATA THAT IS NOT RELATED TO OR IDENTIFIES A NATURAL PERSON, E.G. BUSINESS CONTRACTS ARE NOT COVERED (THOUGH THE AGENTS ARE) BUT THESE WOULD HAVE SEPARATE COMMERCIAL IN CONFIDENCE RULES THAT ARE FOR TLCCH AND THE OTHER PARTY TO NEGOTIATE AND AGREE.

ARE THERE ANY SPECIFIC RULES WE SHOULD BE FOLLOWING TO ENSURE COMPLIANCE?

GDPR SAYS THAT PERSONAL INFORMATION MUST BE	WHAT THIS MEANS
Processed lawfully, fairly and in a transparent manner	At least one of the GDPR conditions allowing the collection, use, sharing, retention of PI must be applied (e.g., contract, legal requirement, legitimate business interest, consent). **CONSENT SHOULD ONLY BE APPLIED IF IT CAN BE WITHDRAWN, THIS IS NOT THE CASE FOR A LOT OF OUR PROCESSING SO WE WILL BE IDENTIFYING ALTERNATIVE CONDITIONS WHERE NEEDED. INDIVIDUALS MUST BE TOLD WHO IS COLLECTING, USING, SHARING, KEEPING THEIR INFORMATION**
Collected only for specified, explicit and legitimate purposes	Personal information must only be used for the purposes it was collected and in line with what the individual was told
Adequate, relevant and limited to what is necessary	Only collect, use, share, hold personal information that's needed for the purpose intended and as explained to the individual
Accurate and kept up to date	Information must be kept accurate and up to date
Held only for the absolute time necessary and no longer	Personal information should only be kept for the time necessary for the purpose it was collected and as explained to the individual in line with the retention policy and standard
Processed in a manner that ensures appropriate security of the personal data	Personal information must be protected, always kept safe and secure

CONSEQUENCES	
Fines	Maximum of €20mn or 4% of global annual turnover whichever higher
Breach Notification	Data breaches must be reported to the ICO within 72 hours
Security	Clear requirements on monitoring, encryption, anonymisation and availability
Data Management	Requirements relating to adequate levels of Operational control which means having a framework for managing Personal Information The accountability of Data Controllers to manage their Personal Information has been strengthened
Legitimacy	Other conditions will be considered and applied and consent only used where no other condition can be applied and the consent can be withdrawn
Consent	Explicit consent is effectively now required which means clear explanation and no pre-ticked boxes
Inventory	An inventory of Personal Information processing activity must be maintained
Privacy Impact Assessments (PIA)	A PIA must be performed where the processing activity is considered “high risk”
Individuals Rights	Have several rights, including the right to request a copy of all their data from a company Additionally have the rights of Data Portability and Erasure
Using Data Processors	Data Processors are now required to comply with aspects of the regulation and can be fined. The Data Controller must conduct due diligence on the processor and maintain oversight of the ongoing adequacy of supplier risk and control management

TLCCH DETAILED GDPR POLICY

1 INTRODUCTION

This Policy sets out the obligations of TLCCH Ltd, a Community Benefit Society ("the Company") registered in England under number 7585 regarding data protection and the rights of data subjects in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is a living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must always be followed by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2 THE DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- 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.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the data subject.

- 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.

RIGHTS OF DATA SUBJECTS

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed (Part 12 Keeping Data Subjects Informed)
- The right of access (Part 13 Data Subject Access)
- The right of rectification (Part 14Rectification of Personal Data)
- The right to erasure (known as the 'right to be forgotten') (Part 15 Erasure of Personal Data)
- The right to restrict processing (Part 16 Restriction of Personal Data Processing)
- The right to data portability (Part 17 Data Portability)
- The right to object (Part 18 Objections to Personal Data Processing)
- Rights with respect to automated decision-making and profiling (Part 19 Personal Data Collected, Held, and Processed)

4 LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

The processing is necessary for compliance with a legal obligation to which the data controller is subject;
The data subject has given consent to the processing of their personal data for one or more specific purposes;

5 SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES

The Company collects and processes the personal data set out in Part 21 of this Policy. This consists of personal date collected directly from data subjects.
The Company only collects, processes, and holds personal data for the specific purposes set out in Part Data Security – Storage of this Policy (or for other purposes expressly permitted by the GDPR).
Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 5 Specified, Explicit, and Legitimate Purposes for more information on keeping data subjects informed.

6 ADEQUATE, RELEVANT, AND LIMITED DATA PROCESSING

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will

be informed) as under Part 5Specified, Explicit, and Legitimate Purposes, above, and as set out in Part Data Security – Storage, below.

7 ACCURACY OF DATA AND KEEPING DATA UP-TO-DATE

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14 Rectification of Personal Data, below.
The accuracy of personal data shall be checked when it is collected and at regular] thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8 DATA RETENTION

The Company shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held, and processed.
When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to Part 20 Data Retention.

9 SECURE PROCESSING

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 23 Data Security – Disposal to 28 Implementation of Policy of this Policy.

10 ACCOUNTABILITY AND RECORD-KEEPING

The Company's Data Protection Officer is, Dave Wardell, DPO@tlchub.org.uk
The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.
The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;

- Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company (please refer to Part 20 Data Retention); and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11 DATA PROTECTION IMPACT ASSESSMENTS

The Company shall carry out Data Protection Impact Assessments for any and all new projects or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- The Company's objectives;
- How personal data is to be used;
- The parties (internal or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to the Company; and
- Proposed measures to minimise and handle identified risks.

12 KEEPING DATA SUBJECTS INFORMED

The Company shall provide the information set out in Part 12 Keeping Data Subjects Informed to every data subject:

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

if the personal data is used to communicate with the data subject, when the first communication is made; or

The following information shall be provided:

- Details of the Company including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13 DATA SUBJECT ACCESS

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
Data subjects wishing to make a SAR may do so in writing. SARs should be addressed to the Company's Data Protection Officer at DPO@tlchub.org.uk.
Responses to SARs shall normally be made within one month of receipt; however, this may be extended by up to two months if the SAR is complex or numerous requests are made. If such additional time is required, the data subject shall be informed.
All SARs received shall be handled by the Company's Data Protection Officer.
The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14 RECTIFICATION OF PERSONAL DATA

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15 ERASURE OF PERSONAL DATA

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 Objections to Personal Data Processing of this Policy for further details concerning the right to object);

The personal data has been processed unlawfully;
The personal data needs to be erased for the Company to comply with a legal obligation
Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
If any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16 RESTRICTION OF PERSONAL DATA PROCESSING

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so)

17 DATA PORTABILITY

The Company processes personal data using automated means.
Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format:
Comma-separated ASCII files.
Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18 OBJECTIONS TO PERSONAL DATA PROCESSING

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for historical research or statistics purposes.
Where a data subject objects to the Company processing their personal data based on their legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override

the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

19 PERSONAL DATA COLLECTED, HELD, AND PROCESSED

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Subject	Collected Data
Members	Name, contact details, start of membership, end of membership, type of membership
Staff	Payroll, tax, working time, role, skill level, appraisal details, and other information as detailed in the employment contract.
Volunteers	Contact information, availability, skills
Supporters	Contact information
Lessees	Information required for the contract
Hirers	Information required for the contract
Enquirers	Contact information and that required to respond to the enquiry

20 DATA RETENTION

Data Subject	Collected Data
Members	For up to three years after your membership ends or longer if required by law
Staff	For up to five years after your employment ends
Volunteers	Until you ask to come off the volunteers list
Supporters	Until you ask to come off the supporters list
Lessees	As required by contract law
Hirers	As required by contract law
Enquirers	Until six months after the query has been answered so we can respond to follow-up questions or as soon as you ask for the information to be deleted.

21 DATA SECURITY - TRANSFERRING PERSONAL DATA AND COMMUNICATIONS

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted using AES encryption;
- All emails containing personal data must be marked “confidential”;
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient;
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

22 DATA SECURITY – STORAGE

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically is stored in secure cloud storage and is automatically backed up;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary;
- Any mobile device on which personal data is held (including, but not limited to, laptops, tablets, and smartphones) must have its storage encrypted and be password protected with the password known only to the device’s owner; and
- Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the

Company that all suitable technical and organisational measures have been taken).

23 DATA SECURITY – DISPOSAL

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

24 DATA SECURITY - USE OF PERSONAL DATA

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer;
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Protection Officer;
- Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it; and
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Secretary to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

25 DATA SECURITY - IT SECURITY

The Company shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Company-owned computer or device without the prior approval of the Data Protection Officer.

26 ORGANISATIONAL MEASURES

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any

costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

27 DATA BREACH NOTIFICATION

All personal data breaches must be reported immediately to the Company's Data Protection Officer.
If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
If a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
Data breach notifications shall include the following information:
The categories and approximate number of data subjects concerned;
The categories and approximate number of personal data records concerned;
The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
The likely consequences of the breach;
Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

28 IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of 1st April 2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Approved: 21/03/2022

Next review 2 years after approval.