佛教慈濟基金會英國聯絡處
Buddhist Compassion Relief
TZU CHI UK Tzu Chi Foundation UK

Data Protection Policy

Purpose

This policy sets out the responsibilities and arrangements within Tzu Chi UK (but excluding the Tzu Chi Academy in London) for meeting its duties in respect of data protection law.

We process personal data in order to deliver our services, recruit and support volunteers, provide information about our work, fundraise, and to operate lawfully in the UK as a registered charity and a registered company limited by guarantee.

Our Aims

We undertake to respect individual privacy; and to only process personal data in accordance with the data processing principles set out in the GDPR. In particular, we will not process any personal data unless we have identified a legal basis on which to do so.

Accountability and Governance

Responsibilities

1. Overall responsibility for ensuring that Tzu-Chi UK meets its legal duties as the data controller rests with the trustee board. Accordingly, compliance with data protection law will be an item in the trustees' risk register.

2. Day-to-day operational compliance will be overseen by our Data Protection Compliance Support Volunteer (DPCSV): Hsin-Ling Liang. She will ensure that that volunteers understand and follow the necessary arrangements that have been put in place to respect privacy and process personal data lawfully in accordance with the GDPR principles. She will keep appropriate documents (see below) and report to the trustee board on progress with maintaining compliance.

3. Volunteers are responsible for following instructions and policies to ensure the security and lawful processing of any personal data.

Documentation

Tzu Chi UK will keep a record of all documentation that demonstrates compliance with data protection law, including any forms, notes, reports or contracts created in respect of the arrangements set out below.

Arrangements

Data Processing Audit

All data processing operations will be audited to establish the nature of any personal data that is being processed, the purpose of the processing, the method in which it is processed; and the nature of any privacy risk associated with the processing.

The information from the data audit will be used to identify a lawful basis for the data processing; to create and modify as appropriate, our Privacy Policy; and to take appropriate measures to ensure the security of the personal data concerned.

Data audits will be reviewed every three years or earlier if there is any change in the method or purpose of the data processing, if there is a complaint made about the processing, or if there is a data breach.

Privacy Risk Assessment

The overall volume of personal data we process is low and most is considered by us to be of low privacy risk. However, we have identified that the processing of some personal data that is considered by us as having a higher privacy risk. These are criminal records checks for volunteers (through the Disclosure and Barring Service); and the sensitive health/medical conditions of service users. In such cases, confidentiality and secure processing are applied. The correct handling of such data is also covered in volunteer inductions and training.

We strive to ensure that physical and cyber access to all our personal data is secure (see below: Data Security Measures).

Privacy Policy

A privacy policy will be published on the Tzu Chi UK website; and will be drawn to an individual's attention whenever personal data is collected. This may involve providing a paper copy of the policy and/or publishing a short privacy statement at the point of data collection, including on any data collection forms, with a reference or link to the full policy.

Data Storage

Personal data will only be kept for as long as it is needed. We store personal information securely using the following cloud-based services: Google Workspace, Business One Drive, and Jotform. The appropriate internal form should be used by volunteers when recording such data; and it should be uploaded at the earliest opportunity. Service users' information is

kept for a further two years after service delivery has ended, after which it is erased. Volunteers' information is subject to annual renewal.

Photos and videos may be kept indefinitely for promotional purposes.

Data Sharing Arrangements

In accordance with our Privacy Policy, personal data may be shared with or obtained from other organisations. We only share information when it is necessary, such as to benefit or improve the wellbeing of the individual concerned through a referral to a specialist agency or if an individual wants to move to another international branch of Tzu Chi or to work for an overseas charity.

We may also share via WhatsApp, photographs or videos of volunteers or service users with Tzu Chi headquarters in Taiwan.

We only transfer data where we are sure that the receiving data controller will respect privacy and in the case of UK based organisations, process data in accordance with the law. This will include being confident that the receiving organisation has in place suitable data security measures (see below: Data Security Measures; and clause 12 in the appendix to this policy)

Where online services are provided by third parties (e.g. PayPal, Galabid, Jotform) we enter into a formal user agreement with such organisations.

We normally obtain explicit consent from the individuals' concerned before transferring personal data (including for photographs and video) unless we are required to share information for specific legal reasons (e.g. to prevent or detect a crime), to safeguard a child or an adult at risk, or to protect life.

For criminal records checks on our volunteers, we send personal data provided by the individual concerned to the Disclosure and Barring Service (DBS) via a third-party umbrella organisation, Aaron's Department Limited. They are authorised by the UK Government to act as an intermediary between the DBS and other organisations and they have *Cyber Essentials* certification. For volunteers working in regulated activities, the processing of data in this way is necessary to comply with the law, and additionally, requires the individual to give their consent to the DBS check.

For referrals and DBS checks, the appropriate internal form will be used and sent via email or other method agreed with the recipient organisation (e.g. using a file transfer service).

Training

We will ensure that volunteers responsible for processing personal data are appropriately trained on how to carry out such duties in a secure manner; and in accordance with the arrangements set out in this policy.

Special Category and Criminal Records Data

For the delivery of certain services it may be necessary for us to collect personal data regarding an individual's health and medical conditions. We also need to collect criminal records data in the form of a Disclosure and Barring Service (DBS) check. In all cases, in addition to the lawful basis, the additional condition we apply for data processing is to receive the individual's consent.

Photographs and video

From time to time, we may seek to take photographs or video of volunteers or people attending our events; and use these for marketing purposes, including on social media. We will obtain the explicit consent of an individual with our "Photography and Interview Consent form" before taking a photograph or recording them.

Upholding Individual Rights

Any complaint or requests about the handling of an individual's personal data, including data access requests) will be dealt with under the following procedure:

1. Individuals will be asked to submit in writing their complaint or request concerning the processing of their personal data. Upon receipt it will be referred immediately to the Data Protection Compliance Support Volunteer (DPCSV).

2. The complaint or request will be investigated; and where upheld, remedial action will be taken and the individual concerned will be notified. If the complaint is not upheld or the request is refused, the DPCSV will notify the individual in writing, explaining the reasons, and will advise them of their right to take-up the matter further with the Information Commissioner's Office.

3. All requests for access to personal data, or other requests/complaints will be dealt with and responded to within the timeframes set out by law.

Procedure for Dealing with a Data Breach

All potential data breaches are taken seriously; and the following procedure will be used:

1. We will investigate any breach of individual privacy as a matter of urgency. This will be undertaken by the Data Protection Compliance Support Volunteer (or in her absence, a trustee) and the trustee board will be informed.

2. We will consider whether the breach poses a risk to individuals, their rights and freedoms, including possible emotional distress, physical and/or material damage. If any of these are likely, those affected will be informed without delay.

3. Action will be taken at the earliest opportunity to mitigate the breach.

4. The Information Commissioner's Office and the Charity Commission will be notified within 72 hours of the breach, unless there is no risk to individual rights and freedoms.

5. A record of the breach and any subsequent actions taken will be recorded and reported formally to the trustee board.

6. Operating procedures and protocols, together with data security measures, will be reviewed and improved to prevent any further such breach.

Data Security Measures

We will ensure that personal data is processed securely. Measures will be taken to prevent loss, theft or other damage to personal data; and to enable data recovery in the event of a security breach.

Volunteers will be trained on appropriate cyber security measures; and we will seek expert advice where appropriate.

Organisations to whom data is transferred will be asked to confirm that they have sufficient data security measures in place to protect the privacy of individuals.

A summary of the measures we take is set out in the appendix to this policy.

Review of this policy

The trustees will review this policy and current cyber security measures every three years, immediately following a data audit.

Date Policy Agreed by Trustees:
Chien Lung Chu, Liang Phik Jenny Lie, Pi Yen Peng, Fen Yauw Frank Lie

Date Next review to commence:
December 2026

Appendix: Data Security Measures

1. All personal data will be uploaded on the correct form at the earliest opportunity to the appropriate cloud-based service that we use: Google workspace; Business OneDrive and Jotform. Once uploaded, any hard copies of notes will be destroyed. Referral forms and case notes are prohibited from being downloaded onto volunteers' personal devices.

2. Only those involved in reaching a decision about cases will be given reading access to completed forms and case notes. This includes members of the Charity Support Team and the Executive Committee.

3. Take extra care in public places. Do not allow screens on any of your devices to be viewable by anyone who is not a Tzu Chi UK volunteer.

4. All laptops and desktop devices used for our work that can connect to the Internet must have current anti-virus software installed. Updates and patches of such software must be installed when made available.

5. Where available, laptop or desktop firewalls must be installed and operational.

6. Updates and patches to operating systems of any mobile device (ie. phones and tablets) used for our work that connect to the internet must be installed at the earliest opportunity.

7. Where possible, laptops should be encrypted.

8. When connecting to the Internet, volunteers should not use an unsecure network. Public WiFi that is not secure must not be used. Instead connect using your mobile data network (4G or 5G), tethering laptops and other devices to your mobile phone if necessary.

9. Online user accounts/log-in details must use a robust password. For example, these should be made up of three random words, using upper and lower case letters, at least one number and a symbol. Pet's names, dates of birth, and other common types of password must not be used.

10. Do not download onto your devices any apps or other software from a third-party vendor. Go to an official app store or the website for the software itself. Do not download any file if you have doubts as to its safety or authenticity.

11. All volunteers should learn how to spot a phishing email (bogus, fake or other suspicious email). Such emails should not be answered under any circumstances.

12. If making a personal data transfer to a third-party organisation for the first time, you should check in advance with our Data Protection Compliance Support Volunteer that it is safe for the transfer to go ahead. (Personal data must not be transferred unless Tzu Chi is satisfied the receiving organisation has sufficient data security measures in place to protect privacy).

13. All volunteers must report any suspected cyber or other data security breach to our Data Protection Compliance Support Volunteer.

14. All devices must be stored securely when not in use. They should not be left in public venues where they might easily be stolen.