THURROCK CENTRE FOR INDEPENDENT LIVING (TCIL) DATA PROTECTION POLICY

Introduction

We hold personal data about our Data Subjects and other individuals for a variety of organisational purposes in the day-to-day running of the Company. As a Company Limited by Guarantee and a Disabled Persons' User-Led Organisation (DPULO) we provide advice, information, guidance, advocacy support for Disabled People, Older People, their families and carers across Thurrock.

This policy sets out how we seek to protect personal data and ensure that Directors, Employees and any volunteers understand the rules governing their use of personal data to which they have access in the course of their role. In particular, this policy requires Directors to ensure that the Board of Directors be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Organisational purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - The maintaining of a database of individuals who have contacted Thurrock Centre for Independent Living (TCIL) for information, advice, guidance or advocacy. - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring organisational policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording minutes, attendance, transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing Directors, Employees and Volunteers access to systems and facilities, administration and assessments - Monitoring Directors, Employees and Volunteers conduct, disciplinary matters - Marketing and publicising our organisation - Improving services - Providing a payroll service to specific local not-for-profit organisations

Personal Data	Information relating to identifiable individuals, such as individuals to whom we have provided advice, information, guidance, advocacy support, current and former Directors, suppliers and marketing contacts. Personal data we gather will include: • *The First Name and Last Name of An Individual* • *The organisation for whom the individual work or represents* • *The individual's email address* • *The individual's contact telephone number* Individuals are asked to positively opt-in (consent) to the processing of the above data in relation to the outcomes and associated paperwork of the specific support they have received, and wish to be kept informed of progress and developments thereto.
Sensitive personal data	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, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all Directors, Employees and Volunteers. You must be familiar with this policy and comply with its terms.
This policy supplements our other policies relating to safeguarding and equal opportunities. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to Directors, Employees and Volunteers before being adopted.

Who is responsible for this policy?

Our Directors have overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

Director's responsibilities:

- Keeping the Thurrock Centre for Independent Living (TCIL) Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from Directors, members and other stakeholders

- Responding to individuals such as Directors and individual "data subjects" who wish to know which data is being held on them by Thurrock Centre for Independent Living (TCIL)
- Checking and approving with third parties that handle the organisation's data any contracts or agreement regarding data processing
- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the organisation is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the Thurrock Centre for Independent Living (TCIL) Board of Directors to ensure all marketing initiatives adhere to data protection laws and the organisation's Data Protection Policy

The processing of all data must be:

- Necessary to perform our aims and objects as a Company Limited by Guarantee and a Disabled Persons' User-Led Organisation (DPULO)
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

We have produced a Privacy Notice to individuals on data protection.

The notice:

- Sets out the purposes for which we hold personal data on individuals, Directors, Employees and Volunteers
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that individuals, Directors, Employees and Volunteers have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive , given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Board of Directors.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform a Director so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Board of Directors will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all Directors to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The TDN Board of Directors must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the organisation's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Board of Directors.

Subject access requests

Please note that under the General Data Protection Regulation (GDPR), individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the Board of Directors. We may ask you to help us comply with those requests.

Please contact the Board of Directors if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Board of Directors about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the Board of Directors for advice on direct marketing before starting any new direct marketing activity.

Training

All Directors, Employees and Volunteers will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	

Who is collecting it?	
How is it collected?	
Why is it being collected?	
How will it be used?	
Who will it be shared with?	
Identity and contact details of any data controllers	
Details of transfers to third country and safeguards	
Retention period	

Conditions for processing

We will ensure any use of personal data is justified using two of the conditions for processing and this will be specifically documented. All Directors, Employees and Volunteers who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record (Disclosure & Barring Service – DBS) checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Board of Directors will be responsible for ensuring that Privacy Impact Assessments and ensuring that all IT projects comply with this policy.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the Board of Directors. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All Directors have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring
Everyone must observe this policy. The Board of Directors has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Board of Directors by calling 01375 389 864 or by email kellybacon@tcil.org.uk