Registered Charity No.1192282

Data Protection and Confidentiality Policy & Guidance

Approved by Trustee Board: March 2025

Next Review: April 2028

Policy

Together We Can Do recognises our responsibilities under the General Data Protection Regulations (GDPR) with respect to the processing of personal data and protecting the rights and privacy of all living individuals to avoid causing harm by the unauthorised disclosure of information.

To achieve this we will

1. Obtain personal data only for specified and lawful purposes.
2. Ensure that such personal data (both written and computerised) is not processed in a manner that is incompatible with the purpose for which it was obtained.
3. Ensure that personal data is adequate, relevant and not excessive for the purpose for which it is held.
4. Ensure that personal data is accurate and kept up to date.
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure and destroyed when it is no longer required.
7. Ensure that personal data is not disclosed or shared with a third party without written agreement.
8. Appoint an individual to undertake a “Data Protection Officer” role to ensure that good data protection practice is adopted and to address any concerns regarding the management and disclosure of data.
9. Provide training and support for all staff and volunteers who handle personal data.
10. Ensure that staff and volunteers read and accept any policies and procedures that relate to the personal data they may handle in the course of their work.
11. Ensure that any breaches of this policy are investigated and reported to the relevant authorities where appropriate.

Responsibilities

The Trustees are responsible for

1. Appointing a suitable individual to provide advice on the management and processing of data held by the charity.
2. Ensuring that members (beneficiaries, staff, volunteers and trustees) are provided with information setting out the charity's expectations relating to handling and storage of personal data.
3. Monitoring the performance of the organisation's data protection policy and initiating action to address any potential non-compliance with legal requirements.

The Data Protection Advisor responsible advising the trustees on its data protection obligations and assisting the organisation to monitor internal compliance. The advisor is responsible for

1. Advising the trustees on data protection matters and draft associated policies and procedures.
2. Identify, organise and where appropriate deliver training to trustees, hired staff and volunteers on data protection matters.
3. Define and review at least every 6 months the Data Register.
4. Act as the contact point for data subjects and respond to requests made by data subjects.
5. Keep a record of all personal data breaches and ensure that they are reported to the trustees and other relevant bodies where necessary
6. Ensure that appropriate measures to reduce the risk of reoccurrence of a data breach are identified and implemented.

Guidance

Data Protection Principles

There are six Data Protection Principles defined in Article 5 of the GDPR. These require that all personal data be:

- Processed in a lawful, fair and transparent manner.
- Collected only for specific, explicit and limited purposes (‘purpose limitation’).
- Adequate, relevant and not excessive (‘data minimisation’).
- Accurate and kept up to date where necessary.
- Kept for no longer than necessary (‘retention’).
- Handled with appropriate security and confidentiality.

Use of Data Processors

Only processors who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected are used.

Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this will be taken into consideration for choice of supplier.

Where a data processor is used then a written contract with compulsory terms as set out in Article 28 of the GDPR must be in place (plus any additional requirements that the charity may determine).

Good Working Practice

Adoption of the following will help protect personal data and ensure compliance with this policy. This guidance should be read in conjunction with the charity’s IT and Social Media Policy and Guidance

- Know what the data protection principles are and apply them. If you have a question about any data protection issue, ask the Data Protection Advisor (Joanne Martin).

- Always treat people’s personal information with integrity and confidentiality. Don’t hand out personal details just because someone asks you to do so.

- Personal data collected and shared should be the minimum amount possible. Where possible personal data should be anonymised and pseudonymised when stored or transferred.

- Only the data that is necessary to fulfil the legal purpose of sharing with an authorised third party should be disclosed.

- Retain personal data for only as long as it is necessary to meet its purpose.

- Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where anyone could access it. Hard copies should be transferred directly to recipients.

- Use an encrypted USB drives to store and transfer data. No other removable media devices should be used to transfer personal data / information.

- Take care when connecting to public wi-fi connections, as these can expose your connection to interception. If you're not sure if a connection is secure, do not connect to it.

- Use your organisational email address, rather than send data to your personal email. Take care to email the intended recipient (especially where email address autocomplete is turned on). Use the 'bcc' field for emailing several people.

- If you are thinking of sending marketing to individuals, consult with the DPO first, as there are certain laws that apply to electronic direct marketing. This could include anything that promotes the aims or purpose of TWCD, including promoting an event or seeking engagement.

- These procedures and policies also apply to the use of remote access to TWCD cloud systems. If you are using your own device to access personal data on cloud-based systems (e.g. Outlook or Gmail) then ensure that your device has a firewall and is password protected.

- Be alert to cyberattacks and report suspicious emails or calls.

Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper
- hacking or other forms of unauthorised access to a device, email account, or the network
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
- alteration or destruction of personal data without permission

These should be reported as soon as possible to the DPO.