



Ment4 Data Protection Policy

Last updated	21.01.25
--------------	----------

Definitions

Organisation	Ment4, the trading name of Teen Crisis UK
GDPR	means the General Data Protection Regulation.
Responsible Person	Luke Peters (prime) Joanna Joseph (secondary)
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.

SEE APPENDIX FOR SPECIFIC PROCEDURES ADOPTED BY MENT4:

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. 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;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. 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;
- e. 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; and
- f. 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.”

2. General provisions

- a. This policy applies to all personal data processed by the Charity.
- b. The Responsible Person shall take responsibility for the Charity’s ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.
- d. The Charity shall register with the Information Commissioner’s Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
- b. The Register of Systems shall be reviewed at least annually.
- c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

- a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).
- b. The Charity shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity’s systems.

5. Data minimisation

- a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

- a. The Charity shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.



7. Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

- a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When documenting information about mentees, it is imperative to employ acronyms to uphold confidentiality standards when communicating with external agencies.
- d. When personal data is deleted this should be done safely such that the data is irrecoverable.
- e. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO ([more information on the ICO website](#)).



APPENDIX

(SPECIFIC PROCEDURES ADOPTED BY MENT4)

TIMELINE OF MENTORING REFERRAL DATA

- Background information and personal details regarding each mentee will be conveyed verbally or via email from referral agencies to Team Leaders or the Director. This information will be securely stored on personal computers or in paper files, which will be under the personal supervision of these individuals and inaccessible to others. Storage will be at their homes in locked cupboards or similarly secure locations. Any computers removed from the designated safe location will be kept under the personal supervision of the owner at all times.
- Before starting the program, mentors will receive internal guidance from Ment4 regarding mentee background and details. While most information will be provided verbally, any written information will utilize initials instead of full names. Additionally, identifying data such as addresses and phone numbers will be sent separately. As a general practice, names of family members and associates will not be disclosed. This will ensure confidentiality is in place.
- Team members are required to maintain strict confidentiality when documenting information related to mentees or their families and associates. Any notes or documents must obscure identities using methods such as initials. If there is a need to retain identifying data, it will only be done with the permission and guidance of Team Leaders.
- Mentors are instructed not to retain photographs of individuals unless explicitly instructed by higher authorities overseeing the mentees, and with approval from Team Leaders. The standard practice is to avoid taking photographs that could identify mentees. However, if requested by authorized individuals, photographs may be taken, sent electronically, and promptly deleted after transmission.
- Mentors will send their Weekly Reports to Team Leaders while adhering to the established security protocols. Following review, edited Weekly Reports will be forwarded to referral agencies using the same secure methods. Team Leaders will then provide Weekly Report Summaries to the Director in a similar manner.
- All periodic reporting of outcomes to referral agencies and other general correspondence will adhere to the established security procedures outlined above. Alternatively, encrypted emails may be utilized for added security measures.



DATA STORAGE AND ACCESS RESTRICTIONS

- Personal data identifying individuals will be stored securely in personal files or computers owned by the Team Leaders and Director, following the outlined security measures. Mentors will attempt to avoid holding any data that directly identifies mentees, their families, or associates.
- Any necessary identification of the young person will be minimized through addressing them with acronym, in both through written or digital format, under the guidance of Team Leaders to maintain confidentiality.

COMMUNICATION TO PROFESSIONAL AGENCIES

- All reports will be anonymized as much as possible. Alternatively, encrypted emails may be utilized.
- When emails are dispatched to multiple recipients, they will be sent as BCC to ensure the email addresses of others remain undisclosed.

COMMUNICATION TO MENTEES AND THEIR FAMILIES

- Mentors will prioritize verbal communication wherever possible, seeking written communication only with approval from Team Leaders. Photographs will only be captured if specifically approved by the individuals in charge of the mentee. After transmission, photographs will be promptly deleted, except in cases where there are no identifiable features such as faces, homes, or schools.

COMMUNICATION VIA MAILING LIST

- Individuals will only be added to the mailing list upon consent. Current recipients of the Prayer Mailing list have already provided consent and will not require reconfirmation. However, they will be informed about Data Protection regulations and provided with a clear option to opt out of the list.
- MailChimp will be utilized for mailing purposes as it ensures the anonymity of other recipients.

REMOVAL OF DATA AND DATA SECURITY

- Data identifying individuals will be reviewed and deleted annually, where it is not needed for longer term reporting and statistics.
- All reasonable means will be taken to ensure data is not stolen from Ment4, particularly from computers, phones, texts, social media and emails. Where possible, verbal communication will be used as a preference to written or pictorial data.

‘RESPONSIBLE PERSON’ AND ‘PROCESSOR’



- The 'Responsible Person' is the one who receives the data and they are responsible for its security under this policy. The prime person responsible for the policy and its adherence is the CEO (Andy Stranack). The prime people receiving the data and keeping it secure are the Team Leaders (Nadine Roberson and Natasha Sutherland).
- 'The Processors' are those who use Ment4's data to process it for various purposes. They include the Finance Administrator (Helen Counter), Finance Advisor (Martyn Williams), payroll processors (ePayroll), Mail Chimp, referral agencies, other professional agencies, and may include others in the future. They are to confirm to Ment4 that they comply with this Data Policy, and provide their own data policies to Ment4.

REGISTER OF SYSTEMS

- A register of all systems or contexts in which personal data is processed by Ment4 will be kept and made available to anyone requesting access with reasonable grounds.

REVIEW OF POLICY

- The Director and Team Leaders will review this policy annually and report to the Advisory Board, which includes the Trustees. Records of all data storage matters relating to this Policy will be kept.

The Management of Ment4 endorses and actively supports this policy.

Signed: *Luke Peters, Lead Director, Ment4*

A handwritten signature in black ink, appearing to be "L Peters", is written over a small, light grey rectangular background. To the right of the signature is the Ment4 logo, which consists of the word "MENT" in grey and a red "4" with a small grey figure above it.