



# **Data Protection Policy**

**Last Updated: April 2026**

## Data Protection Policy

### Purpose of this policy

This policy explains how MENT4 collects, uses, stores and protects personal data. It ensures that all information is handled lawfully, safely and respectfully, in line with data protection requirements.

MENT4 works with sensitive information relating to young people, families, staff and partners. Protecting this information is essential to safeguarding, trust and professional practice.

### What is personal data

Personal data is any information that can identify a person, directly or indirectly.

This may include:

- names and contact details
- dates of birth
- addresses
- school or organisation details
- case notes or mentoring records
- safeguarding information
- medical information
- images, videos or recordings
- staff records

Some information is considered sensitive and requires additional protection.

### Core principles

MENT4 handles data in line with key principles. Personal data must be:

- used lawfully, fairly and transparently
- collected for specific and legitimate purposes
- relevant and limited to what is necessary
- accurate and kept up to date
- stored securely
- kept only for as long as necessary
- handled in a way that ensures appropriate security

All staff are responsible for following these principles.

### Collecting information

MENT4 collects information to:

- deliver programmes and mentoring
- safeguard young people
- communicate with families and partners
- monitor progress and impact
- meet legal and funding requirements

Staff must only collect information that is necessary for the purpose.

### Using information

Personal data must only be used for its intended purpose.

Staff must:

- use information responsibly
- not access data they do not need
- not use information for personal reasons
- ensure accuracy when recording or updating information

### Storing information

All data must be stored securely.

This includes:

- using approved systems and platforms
- protecting files with passwords
- keeping devices secure
- locking physical documents where required
- avoiding storage on personal devices or unapproved systems

Staff must take reasonable steps to prevent unauthorised access.

### **Sharing information**

Information should only be shared where appropriate and necessary.

This may include sharing with:

- line managers
- safeguarding leads
- relevant programme staff
- partner organisations
- external agencies where required

Staff must:

- share information on a need to know basis
- ensure there is a valid reason for sharing
- follow safeguarding procedures where relevant
- ensure data is shared securely

Information must not be shared casually or inappropriately.

### **Confidentiality**

Staff must treat all personal information as confidential.

Staff must not:

- discuss sensitive information in public spaces
- share information with unauthorised individuals
- leave documents or screens visible
- send information to the wrong person

Confidentiality is essential to maintaining trust.

### **Data breaches**

A data breach is any situation where personal data is lost, shared incorrectly or accessed without permission.

This may include:

- sending information to the wrong person
- losing a device or document
- unauthorised access to systems
- accidental disclosure of information

All data breaches must be reported immediately to a line manager or relevant lead.

### **Data retention**

Personal data must not be kept longer than necessary.

MENT4 will:

- follow agreed retention periods
- securely delete or dispose of data when no longer needed

Staff must not keep personal records outside approved systems.

### **Rights of individuals**

Individuals have rights in relation to their data, including:

- the right to access their information
- the right to request corrections
- the right to understand how their data is used

Requests relating to data should be handled through the appropriate MENT4 process.

### **Training and awareness**

Staff must:

- follow data protection guidance
- complete relevant training
- stay aware of responsibilities
- seek guidance when unsure

### **Breaches of this policy**

Failure to follow data protection procedures may result in:

- supervision or guidance
- further training
- review of practice
- formal disciplinary action

Serious breaches may have legal consequences.

**Final note**

Handling data responsibly is a core part of MENT4's work.

By protecting information, staff help safeguard young people, maintain trust and uphold professional standards.

*This document has been approved by:*

**Luke Peters**  
**Executive Director**

A handwritten signature in grey ink, appearing to be "L. Peters".

*Helping young people discover what they are MENT4*

**Tel: 07808 595151**

**E-mail: [luke.peters@ment4.org](mailto:luke.peters@ment4.org)**



