

DATA PROTECTION & GDPR POLICY

Mending Lines

Statement of Intent

Mending Lines is committed to protecting the privacy, confidentiality, and security of personal information.

We recognise our responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and are committed to handling personal data lawfully, fairly, securely, and transparently.

This policy outlines how Mending Lines collects, stores, uses, shares, and protects personal information relating to children, young people, families, staff, volunteers, and partner agencies.

Purpose of Data Collection

Mending Lines may collect and process personal information in order to:

- deliver safe and effective provision
 - safeguard children and vulnerable individuals
 - communicate with families and professionals
 - manage referrals and placements
 - maintain attendance and incident records
 - complete risk assessments
 - meet legal and contractual obligations
 - monitor and improve provision
 - comply with health and safety requirements
-

Types of Information Held

Information held by Mending Lines may include:

- names and contact details
- emergency contact information

- attendance records
- referral information
- safeguarding information
- medical or dietary information relevant to support needs
- behaviour and risk information
- incident and accident records
- reports and progress summaries
- staff and volunteer records where applicable

Only information necessary for the safe and effective running of the provision will be collected.

Lawful Basis for Processing

Mending Lines processes personal data under lawful bases including:

- consent
- safeguarding obligations
- legal obligations
- legitimate interests
- provision of educational and wellbeing support

Sensitive information will only be processed where necessary and appropriate safeguards are in place.

Data Storage & Security

Mending Lines takes reasonable steps to ensure personal information is stored securely.

This may include:

- password protected digital systems
- secure cloud storage
- restricted staff access
- locked storage for paper records

- secure disposal of confidential information
- role-based access to sensitive information

Personal information will only be accessed by individuals who require it for legitimate safeguarding, educational, or operational reasons.

Sharing Information

Information may be shared where appropriate with:

- schools
- local authorities
- safeguarding agencies
- emergency services
- social workers
- healthcare professionals
- other professionals involved in supporting the learner

Information will only be shared where:

- consent has been obtained where appropriate
 - there is a safeguarding concern
 - there is a legal obligation
 - sharing is necessary to support the learner safely and effectively
-

Confidentiality

Staff and volunteers are expected to maintain confidentiality at all times.

Confidential information should not be discussed outside professional settings unless there is a safeguarding or legal reason to do so.

Breach of confidentiality may result in disciplinary action or removal from the provision.

Photographs & Media

Photographs or videos of participants will only be used where appropriate consent has been obtained.

Images may be used for:

- promotional materials
- social media
- website content
- funding reports
- community awareness

Parents/carers may withdraw consent at any time.

Data Retention

Records will only be retained for as long as reasonably necessary and in line with legal or safeguarding requirements.

When information is no longer required, it will be securely deleted or destroyed.

Individual Rights

Individuals have rights under UK GDPR including:

- the right to access their information
- the right to request corrections
- the right to restrict processing in certain circumstances
- the right to request deletion where appropriate
- the right to complain to the Information Commissioner's Office (ICO)

Requests relating to personal information should be made directly to Mending Lines.

Data Breaches

Any actual or suspected data breach should be reported immediately to the management team.

Breaches will be investigated promptly and managed in accordance with legal requirements.

Where necessary, breaches may be reported to the ICO.

Monitoring & Review

This policy will be reviewed annually or sooner if:

- legislation changes
- operational practices change
- a significant data breach or concern occurs

Policy Review

Policy: Data Protection & GDPR Policy

Organisation: Mending Lines

Review Frequency: Annual

Next Review Due: Nov 2026