DEDHAM
Therapy Farm

Data Protection Policy

Next Review: September 2026

1. Introduction

This policy sets out how Dedham Therapy Farm CIC protects personal data and ensures compliance with UK GDPR and the Data Protection Act 2018. It applies to all staff, volunteers and Directors.

2. Responsibilities

- All staff must handle data lawfully and securely
- Managers must ensure compliance and oversight
- Directors provide governance and accountability

3. Lawful Processing

Personal data must only be processed where a lawful basis applies. Consent must be recorded unless another lawful basis is relied upon.

Where consent is used:

- It will be clear and recorded is our designated data sheet
- Consent to process data is obtained at point of referral and updated at a minimum annually
- Consent normally lasts for the duration of involvement unless withdrawn earlier
- Consent can be withdrawn at any time by contacting us

Withdrawal of consent will not affect processing already carried out lawfully.

4. Special Category Data

Special category data (health, safeguarding, education) must be:

- Accessed on a need-to-know basis
- Stored securely
- Shared only where lawful

5. Data Accuracy

Records must be kept accurate and up to date. Errors must be corrected promptly.

We take reasonable steps to ensure personal data is accurate and up to date. Individuals are encouraged to notify us of any changes or inaccuracies.

We send out annual data check questionnaires. This is to ensure the information we hold is accurate and to provide opportunity to update/change data on our systems.

6. Data Retention

Data will be retained in line with the organisation's retention schedule and securely destroyed when no longer required.

DEDHAM
Therapy Farm

This Data Retention Schedule sets out how long Dedham Therapy Farm CIC keeps different types of personal data and how it is securely disposed of, in line with the UK GDPR, Data Protection Act 2018, safeguarding requirements, and best practice.

This schedule applies to data relating to:

- Farm Assistants (children and young people)
- Parents and carers
- Staff and volunteers
- Referrers and professionals

Retention periods may be extended where there is an ongoing safeguarding concern, legal requirement, or active investigation.

Retention Schedule

Data Type	**Examples**	**Lawful Basis**	**Retention Period**	**Secure Disposal Method**
Referral & Assessment Records	Referral forms, initial assessments, consent forms	Legal obligation / Public task / Vital interests	**10 years** from end of involvement	Secure electronic deletion / confidential shredding
Therapy & Progress Notes	Session notes, reviews, outcomes	Legal obligation / Vital interests	**10 years** from last session	Secure electronic deletion / confidential shredding
Safeguarding Records	Safeguarding concerns, referrals, incident reports	Legal obligation / Vital interests	**Until subject is 25 years old** or **10 years** (whichever is longer)	Secure electronic deletion / confidential shredding
Attendance Records	Registers, non-attendance logs	Legal obligation / Public task	**10 years** from end of placement	Secure electronic deletion / confidential shredding
Parental / Carer Contact Details	Names, addresses, phone numbers, emails	Consent / Legal obligation	Duration of involvement + **2 years**	Secure electronic deletion

DEDHAM
Therapy Farm

Correspondence	Emails, letters, records of calls	Legitimate interests / Legal obligation	**6 years**	Secure electronic deletion
Complaints Records	Complaints, investigations, outcomes	Legal obligation / Legitimate interests	**6 years** from closure	Secure electronic deletion / confidential shredding
Accident & Incident Records	Accident forms, incident reports	Legal obligation	**10 years**	Secure electronic deletion / confidential shredding
Staff Personnel Files	Contracts, appraisals, disciplinary records	Legal obligation	**6 years** after employment ends	Secure electronic deletion / confidential shredding
Staff Recruitment Records	Applications, interview notes	Legitimate interests	**1 year** (unsuccessful)	Secure electronic deletion
Volunteer Records	Applications, checks, training records	Legitimate interests / Legal obligation	**6 years** after role ends	Secure electronic deletion
Training Records	Safeguarding, data protection, CPD	Legal obligation	**6 years**	Secure electronic deletion
Financial Records	Invoices, payment records	Legal obligation	**6 years**	Secure electronic deletion
Meeting Minutes	Director & team meetings	Legal obligation / Vital interests	**10 years**	Secure electronic deletion / confidential shredding
Website & Marketing Data	Enquiries, mailing lists	Consent	Until consent withdrawn or **2 years** of inactivity	Secure electronic deletion

CCTV / Monitoring Data	Video or system logs, ring doorbell	Legitimate interests	**30 days** unless required for investigation	Secure deletion

7. Access Controls

Access to personal data is restricted to those with a legitimate business need.

- All access to Dedham Therapy Farm CIC data shall be granted based on the principle of least privilege. Users will only be provided with the minimum access to necessary to perform their current job functions. Access is managed role-based access control and requires multi factor authentication.
- Access rights will be reviewed quarterly by data owners (Directors) and unauthorised attempts to bypass these controls will result in disciplinary action.

8. Data Sharing

All data sharing must be lawful, proportionate and recorded.

We may share personal data with:

- Schools and local authorities
- Health and safeguarding professionals
- Regulatory or statutory bodies

Only the minimum amount of personal data necessary for the defined purpose will be shared.
Personal data may be shared internally only with staff who have a legitimate and authorised need to access it.

Externally sharing data. All documents containing personal data must be password protected and initials only used in the body of the email and the subject heading. – Passwords must be sent separately to the document.

Internally – Documents should be saved to the drive and not sent between staff. Initials must be used in internal emails/messaging. Double initials to ensure clarity.

Personal data must only be sent through Dedham Therapy Farm approved devices.

9. Monitoring

Use of email, internet and IT systems may be monitored in line with UK law. Management reserve the right to access staff drives through Microsoft admin dashboard.

We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including but not limited to the following purposes:

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing;

(d) to comply with any legal obligation.

Staff must not use their own personal e-mail account to send or receive e-mail for the purposes of our business. They must only use the e-mail account we have provided. We do not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks.

10. Security

Appropriate security measures are in place, including:

- Password protection (including two step verifications)
- Secure mobile and home working (including admin policy and working from home agreements)
- Malware protection
- Secure use of removable media (only devices issued by Dedham Therapy Farm may be used)
- Use of lock cabinets to store any hard copies or devices that have access to data.

11. Subject Access Requests (SARs)

Requests to access personal data should be made in writing. A Subject data request form will be sent with acknowledgment of data request.

Children 13 years and over will be asked to provide consent for parent to access their data from us.

We will respond within one month.

Data can be accessed for free.

11. AI Use

Scope & Access
AI capabilities may be used only by authorised roles. Responsibilities for AI configuration, use, review, and incident response are assigned to each member and overseen by the DPO. Each AI use case must be recorded and approved through our DPIA process before live use.

Prohibited Use & Human Oversight
The organisation does not use AI to generate treatment plans or to make any decision based solely on automated processing that has legal or similarly significant effects on an individual. AI outputs may inform staff judgment but must be reviewed, challenged where appropriate, and can be overridden.

Data Inputs
Staff must not input special category data or any data likely to identify a living individual into AI tools.

Approved Tools
Only Microsoft 365 Copilot are approved. Microsoft 365 Copilot operates within our tenant and does not

use our content to train foundation models; we will configure data residency, least-privilege access, audit logging, and retention safeguards.

Transparency & Declarations
Where AI assistance materially influences content or outcomes, staff must declare AI assistance (e.g., "AI assisted draft") and ensure individuals are informed in our privacy notices about our AI use and oversight.

Training
Mandatory training covers data classification, special category data rules, Article 22 safeguards and meaningful human involvement, prompt hygiene, and incident reporting.

DPIA
A DPIA is required for each AI use case prior to deployment, evidencing necessity/proportionality and consideration of less risky alternatives

12. Data Security

All suspected data breaches must be reported immediately to management, including the data protection officer. This includes if they suspect their computer may have a virus.

Breaches will be recorded and managed in line with legal requirements.

We use appropriate technical and organisational measures to protect personal data.

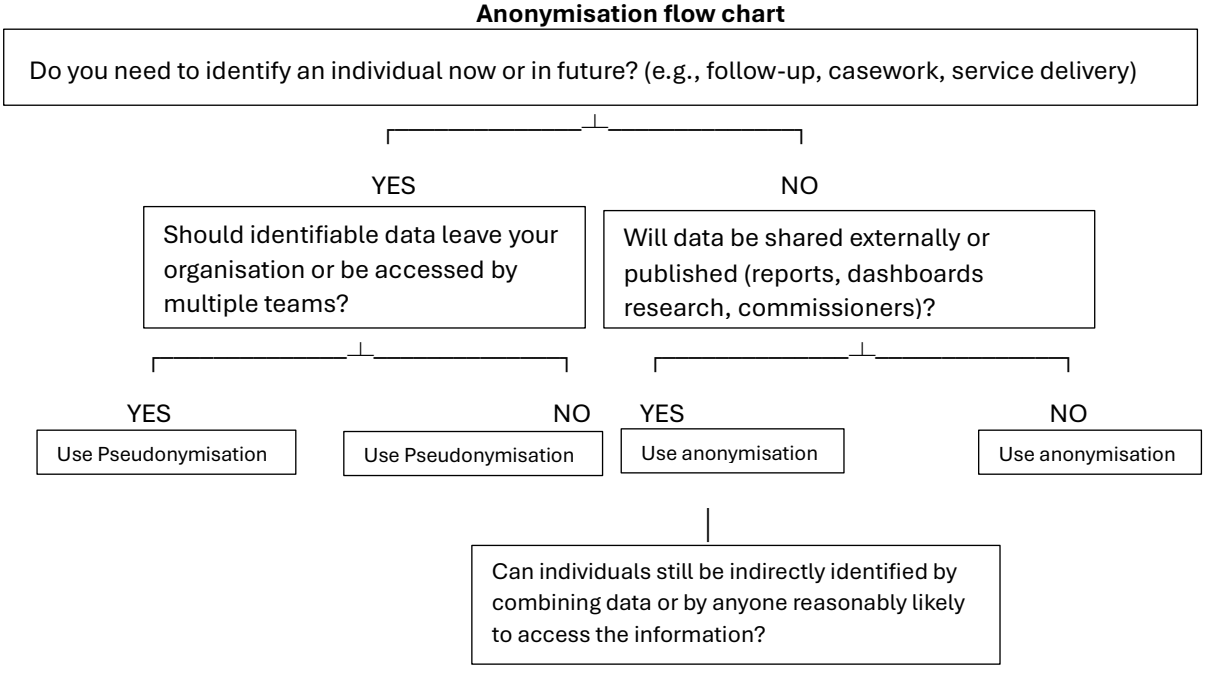
Staff should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

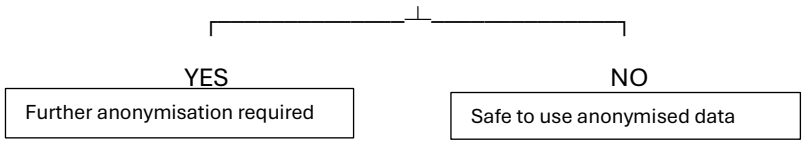
Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware. Staff must not download or install software from external sources without authorisation from management.

Only devices issued by Dedham Therapy Farm CIC can be used or plugged into laptops/computers.

We monitor all e-mails passing through our system for viruses. Staff should exercise caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

Anonymisation flow chart





13.International Transfer

Transferring data outside the EEA is restricted.

If we need to share personal data with an organisations, outside the UK, we must follow strict rules to keep people's information safe. A transfer is only classed as an international transfer when:

- UK GDPR applies to the data,
- it goes to someone outside the UK, and
- that person or organisation is a separate legal entity

What staff must do

- Check first: If the data is going outside the UK, always alert management and or Data Protection Lead.
- We can only transfer data if one of these safeguards is in place:
    - The country is approved by the UK as adequate.
    - We use the correct legal contract
- Before transferring, we must complete a Transfer Risk Assessment (TRA) to make sure the destination country protects data properly

Training

Data protection and GDPR training is mandatory for all staff on an biannual basis.

14. Review

This policy is reviewed annually to ensure ongoing compliance.