Terapia Data Protection Policy

Responsibility of Policy	CEO
Relevant to	All Terapia employees, contractors, trainees, service users, volunteers, business contacts and suppliers
Responsibility For Document Review	CEO
Date Modified	December 2024
Next Review Date	December 2025

This data protection policy relates to obligations under the Data Protection Legislation, which includes the Data Protection Act 2018 (implemented by the General Data Protection Regulations [GDPR])

1. Objectives and Scope of the policy

To ensure that:

- Proper procedures are in place for the processing and management of personal data.
- There is someone within the organisation who has specific responsibilities for data protection compliance.
- A supportive environment and culture of best practice in relation to processing of personal data is provided for staff.
- All staff understand their responsibilities when processing personal data and that methods of handling that information are clearly understood.
- Individuals wishing to submit a subject access request and exercise any of the other individual rights are fully aware of how to do this and who to contact.
- Staff understand that subject access requests (and other relevant requests) need to be dealt with promptly and courteously.
- Individuals are assured that their personal data is processed in accordance with the data protection principles, that their data is secure at all times and safe from unauthorised access, alteration, use or loss.
- Other organisations with whom personal data needs to be shared or transferred, meet compliance requirements.
- Any new systems being implemented are assessed using a Data Protection Impact Assessment to determine whether they will hold personal data, whether the system presents any privacy risks, damage or impact to individuals' data and that it meets this policy's requirements
- This policy applies to all personal data and special categories of data (sensitive personal information) collected and processed by Terapia in the conduct of its business, in electronic format in any medium and within structured paper filing systems.
- This policy applies to all Terapia employees, contractors, or consultants and students.
- Disciplinary action may be taken against staff failing to comply with this policy.
- Terapia is registered with the Information Commissioner's Office (ICO) for collecting and using personal data.

2. The data protection principles and individual rights

The General Data Protection Regulation (GDPR) contains seven "Data Protection Principles" set out in Article 5. These specify that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary.
6. Processed in a manner that ensures adequate security of the personal data, using appropriate technical or organisational measures.
7. Take full accountability for what we do with personal data and how we demonstrate compliance.

Article 5(2) also sets out an overarching accountability principle 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'

Individual rights are set out in a separate part of the GDPR. In brief, the GDPR provides the following rights for individuals depending on the circumstances (further detail on the individual rights listed below can be found in the ICO website):

- The right to be informed – Individuals have a right to be informed on how their data is being used, what the purpose is and the retention periods).
- The right of access – Also known as a Subject Access Request, individuals have a right to their own personal data.
- The right to rectification – Individuals have the right to have inaccurate information corrected.
- The right to erasure – Also known as the right to be forgotten, individuals have the right to have their data erased.
- The right to restrict processing – Individuals have the right to request their data be restricted.
- The right to data portability – Individuals have the right to their data being moved, copied and transferred to another IT system.
- The right to object – In certain circumstances individuals have the right to object to the processing of their data.
- Rights in relation to automated decision making and profiling. – Individuals have the right to know when automated decision making and profiling occurs, and have the ability to request for human intervention or challenge a decision.

3. Policy Principles

In order to meet the requirements of the data protection principles and individual rights set out in the GDPR, Terapia adheres to the following values when processing personal data:

3.1 Fair Collection and Processing

- The specific conditions contained in Article 6 and 9 of the GDPR regarding the fair collection and use of personal data will be fully complied with;

- Individuals will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection through relevant privacy notices;

- Personal data will be collected and processed only to the extent that it is needed to fulfil business needs or legal requirements;

- Personal data held will be kept up to date and accurate, where necessary;

- Retention of personal data will be appraised and risk assessed to determine and meet business needs and legal requirements, with the appropriate retention schedules applied to that data;

- Personal data will be processed in accordance with the rights of the individuals about whom the personal data are held;

- It is important that we determine a lawful basis for processing any personal data. because the lawful basis for processing has an effect on individuals' rights;

- A 'cease processing request' (erasure request from an individual will be acknowledged within 3 working days, with the final response within 21 days. The final response will state whether Terapia intends to comply with the request and to what extent, or will state the reasons why it is felt the requestor's notice is unjustified;

- Staff will advise the Data Protection Officer in the event of any intended new purposes for processing personal data. The Data Protection Officer will then arrange for a Data Protection Impact Assessment to be conducted.

3.2 Security

- Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place;

- Staff will report any actual, near miss, or suspected data breaches to the Data Protection Officer for investigation. Lessons learnt during the investigation of breaches will be relayed to those processing information to enable necessary improvements to be made. The Data Protection Officer will report any 'serious' breaches to the Information Commissioner's Office as necessary, within 72 hours of the breach being reported internally;

- Any unauthorised use of corporate email by staff, including sending of sensitive or personal data to unauthorised persons, or use that brings Terapia into disrepute will be regarded as a breach of this policy;

- Relevant Data Protection Awareness Training will be provided to staff to keep them better informed of relevant legislation and guidance regarding the processing of personal information. Data protection training will also promote awareness of Terapia's data protection and information security policies, procedures and processes. The Data Protection Officer may also advise existing staff who have caused a data breach, or who have otherwise failed to comply with data protection law, or any aspects of the Terapia's data protection policies, to retake the data protection awareness training. The Data Protection Officer may advise staff on any training that may be useful to address any specific training needs of teams or of individual staff.

3.3 Sharing and disclosure of personal information

Regular information sharing with third parties, where there is a valid business reason for sharing information, shall be carried out under a written agreement setting out the scope and limits of

sharing. Data Processing Agreements will be applied to all contracts and management agreements where Terapia is the data controller contracting out services and processing of personal data to third parties (data processors). These agreements will clearly outline the roles and responsibilities of both the data controller and the data processor;

- All data processors shall agree to conform to this policy and the GDPR and as far as possible, indemnify Terapia against any prosecution, claim, proceeding, action or payments of compensation or damages without limitation and provide any personal information specified on request to the Data Protection Officer;

- As part of all relevant privacy notices Terapia will inform individuals of the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the GDPR and other relevant legislation;

3.4 Access

- Members of staff will have access to personal data only where it is required as part of their functional remit;

- Staff are made aware that in the event of a Subject Access Request being received in Terapia , their emails may be searched and relevant content disclosed, whether marked as personal or not;

- A relevant contact address will be made available on the internet for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how Terapia is processing their data, or about our handling of their request for information;

- A Subject Access Request will be acknowledged and the final response and disclosure of information (subject to exemptions) will be given within the timescales required under the within 1 calendar month;

- A data subject's personal information will not be disclosed to them until their identity has been verified;

- Third party personal data will not be released by Terapia when responding to a Subject Access Request or Freedom of Information Request (unless consent is specifically obtained, obliged to be released by law or necessary in the substantial public interest);

- All data subjects have a right of access to their own personal data. Advice will be provided to data subjects on how to request or access their personal data held by the University.

4. Links with the Freedom of Information Act 2000

- The Freedom of Information Act 2000 enables greater public access to information processed by public bodies. However, personal data continues to be protected by the GDPR, and is therefore exempt from disclosure under the Freedom of Information Act (Section 40).

5. Data Protection responsibilities

Data Protection Officer: Jonathan Block Email: DPO@Terapia.co.uk	Terapia, The Bothy, 17A East End Road, Finchley, London N3 3QE

Who	What
Board of Governors	Ultimately responsible for compliance with the GDPR.
Data Protection Officer	• Maintain Terapia's notification with the ICO; • Advise staff on data protection compliance; • Coordinate responses for subject access requests; • Report any personal data breaches to the ICO/police as appropriate; • Issue data sharing guidance. • Develop, administer, disseminate, review and support application of the policy.
All staff	• Be familiar with and comply with the policy; • Ensure that information provided in connection with employment is up-to-date and accurate; • Observe and comply with the data protection principles and individuals data protection rights; • Bring queries and issues around data protection to the attention of the Data Protection Officer; • Do not attempt to gain access to information that is not necessary to hold, know or process; Note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases
All students,	• Be familiar with the policy and comply with the policy where necessary. • Ensure that personal information provided is up-to-date and accurate. • Observe and comply with the data protection principles and individuals data protection rights. Note that unauthorised disclosure of personal data will usually be a disciplinary matter.

Appendix 1: Data Retention at Terapia

GDPR requires personal data not to be retained for longer than we are required to by law or for longer than reasonable.

There are a number of different reasons why Terapia retains data, e.g. the data subject may have accessed our services (training or therapeutic) or they may have been a fundraiser or a volunteer) and there are different data retention periods accordingly.

Financial data

We are required by law (Companies Act and HRMC Inland Revenue for statutory, tax and anti-money laundering purposes) to maintain certain data regarding the financial transactions that we process with individuals for a period of at least 7 years. Therefore if there are valid transactions within this timeframe then we will not be able to erase data relating to these including the basic details of the individual concerned.

Unless we have a valid reason to retain financial data relating to individuals we will delete this after 7 complete financial years have elapsed.

Accessing our services

When prospective clients contact Terapia for our therapeutic services or potential students for training we obtain personal data. This usually includes information such as name, address, date of birth, and contact details. Additional specific information is gathered for students, which may include experience and qualifications. Referrals to our therapeutic service will provide personal information which mayinclude some details of issues faced, other services involved and concerns. All of this data willbe treated with sensitivity, restricted to only relevant personnel and kept confidential.

Where initial enquires from prospective students do not lead to them taking up a place on a course, records will be kept for three years. When prospective clients do not take up a service then we will delete records after one year.

Terapia training courses

Once a Terapia trainee commences training more data will be gathered - this includes but is not confined to academic records, information to obtain enhanced DBS checks, attendance records, and marks obtained. Unless specifically requested otherwise this information will be kept for 10 years after completing or exiting from our training

Bothy Therapeutic Services

When Terapia finishes work with a client we 'close' all paper files and forms, including questionnaires, will be destroyed confidentially at this point. From then we retain the following:

- Names, dates of birth, contact details, and when we started and finished work. We keep this information securely on our database and it is never scheduled for deletion.
- Notes of what sessions took place and with whom. *This data will be kept for 7 years after therapy ends (for adults) and 7 years from a child oryoung person's 18th birthday i.e when they reach the age of twenty five years.*
- Therapeutic materials produced during therapy will be given to clients or an agreementwill be made about how to dispose of them.

- Trainee therapists will destroy any recordings or other specific information made when their training is complete.

Therapeutic services delivered as part of projects in partnership with other organisations,such as schools or other community services.

Data will be kept in line with the host organisations data protection and retention policies. Trainee therapists will keep non-identifiable notes and records until they complete their training. Any identifiable information they hold (which is always kept separate from clinical notes) will be immediately destroyed when their placement finishes.

Staff Records

All of the following staff data is kept for 7 years:

1. Brief staff details such as contact details, the position in which the staff member wasemployed.
2. The financial details, including payroll and pension details.
3. All other staff details, including staff notes, disciplinary proceedings, correspondence,etc.

Fundraising and volunteers

Personal and financial information about supporters (fundraisers and/or volunteers) will be retained as long as there is an association with Terapia. Unless there is an express request to be forgotten, details of supporters will be kept for 7 years after last contact.

Appendix 2: Data Subject Access

- Data subjects may make Subject Access Requests ("SARs") at any time to find out more about the personal data which Terapia holds about them, what it is doing with that personal data, and why.
- Data subjects wishing to make a SAR must do so in writing. SARs should be addressed to Terapia's Data Protection Officer.
- Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the Data Protection Officer.
- Terapia does not charge a fee for the handling of normal SARs. Terapia reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requeststhat are manifestly unfounded or excessive, particularly where such requests are repetitive.

Appendix 3:

Data Security. Transferring personal data and communications

Terapia shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All mobile devices are password protected.
- All emails are marked with a privacy notice stating the confidentiality of the data contained within. Any emails containing sensitive or detailed personal data must be marked "private and confidential" in the subject line and on receipt any relevant personal data contained within must be removed from the email, stored in the appropriate location and the email deleted by all parties The type of data held is then governed by the appropriate retention schedule – for example in relation to staff records, HR records and so on. In the event of a SAR emails containing personal data will be disclosed.
- In general, emails should not be retained longer than is necessary and should be deleted/archived in line with Terapia policy on email retention.
- Personal data may be transmitted over secure networks only; transmissionover unsecured networks is not permitted in any circumstances.
- Where personal data is to be transferred in hard copy form it should be passed directly to the recipient or sent using a secure courier service. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a secure suitable container.

Data Security: Storage

The following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data are stored securely on our file servers and in Dropbox or Microsoft Teams). Access to file servers and databases are password protected. Data in transmission is encrypted using SSL (Third Party Authenticated) and 'at rest' data is encrypted according to the Cloud provider's security standards. Terapia uses Sophos Endpoint Security which includes Firewall, Antivirus and Antispyware software.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar; separating out identifiable and non-identifiable data wherever possible.
- Hardcopies of personal data must not leave office bases unless there is a specific reason to do so and measures have been taken to keep it secure, for instance identifiable and non-identifiable material has been separated. Wherever practicable and possible, employees and volunteers should only refer to personal data via secure routes and on equipment provided by Terapia.In the event that hardcopy data is required outside of the office it should be returned, secured or destroyed at the earliest convenience.
- Personal data must not be transferred to any device personally belonging to an employee and personal data may only be transferred todevices belonging to agents, contractors, or other parties working on behalf of Terapia where the party in question has agreed to comply fullywith the letter and spirit of this Policy and GDPR (which may include demonstrating to Terapia that all suitable technical and organisational measures have been taken).
- Terapia operates a 'clear desk' policy. When not in use any files, folders or documents must be locked away securely. Files or documents containing personal data must never be left unattended. Staff should ensure that personal data they are viewing on their PC or laptop screens cannot be viewed by others.