Nest Play Therapy

GDPR Policy

Policy in effect from:	November 2025
Date of next review:	November 2026
Policy written by:	Debbie Moore

Introduction

Data held by Nest Play Therapy will be held lawfully and for the retention periods set out in this policy document.

Data in document refers to:

- Written Documents
- Spreadsheets
- Hardcopy case notes and files
- Images
- Emails
- Text messages
- Supervision notes
- Visits to the organisation's website
- Social media communication

Aim and Purpose

The purpose of this document is to ensure that Nest Play Therapy has a framework that ensures the rights and freedom of individuals in relation to their personal data (Article 1) and adheres to best practice in the management of client information and business records.

Information Governance sets out the way in which information collated by an organisation is managed and ensures that any information collected;

- is the right information
- is in the right place
- at the right time
- with the right people
- for the right reasons

This is a live document and may be updated at any time to reflect changes in law or growth of the business, and therefore should be revisited regularly to check for any updates. Nest Play Therapy is fully committed to ensuring clients privacy and data protection rights.

For the purpose of this policy Debbie Moore is the named Data Protection Officer/Controller and Head of Organisation.

Information Governance Framework Principles

- Assessment needs for Information Governance (IG) Training have been identified and fully met. Refresher training is completed every two years.
- Any changes to the business processes and/or operations will be planned and will comply with the framework to ensure any risks to personal and sensitive information are minimised.
- Any data collected is solely for the purpose of providing a person-centred service to an individual client. If you collect data for any other purpose you will need to note it here
- The Caldicott Principles are used to provide guidance in best practice when handling personal data, alongside the ICO's Office Codes of Practice. (https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx)
- All records are identifiable, locatable, retrievable, and intelligible according to regulations set out by GDPR.
- It is the responsibility of the Data Controller to ensure sufficient resources are in place to prioritise adhering to Data Protection Legislation in the business.
- Any electronic devices where personal or sensitive, confidential information is held will be password protected.
- Procedures have been put in place to ensure the General Data Protection Regulations are met.

Privacy Notice: Use of Information

In accordance with this data retention schedule there may be occasions when data is not destroyed due to ongoing investigation, ligation or enquiry. The data will be deleted upon confirmation that it is no longer required.

- Personal information is collated and stored in hardcopy in a locked filing cabinet behind a locked door.
- Any document containing personal data will state "Official-sensitive, private and confidential" clearly.

Website visitors

When an individual visits, I use Google analytics who are considered a third party service, to collect information about what visitors do when they click on my website, e.g. which page they visit the most. Google analytics only collect non-identifiable data which means I or they cannot identify who is visiting. Nest Play Therapy will always be transparent when it comes to collecting personal data and will be clear about how that data is processed. Google analytics privacy notice can be found here: https://policies.google.com/privacy/update?hl=en

Wordpress

Wordpress is a third-party service that hosts Nest Play Therapy's website. Wordpress also uses anonymised data to collect visitor information such as how long an individual remains on a page of a website.

Retention Schedule

Information Asset	**Information Owner Asset**	**Retention**	**Trigger for Disposal**
Email (including sent items)	Head of organisation	Annual review period every January, any remaining live data untouched until following review period.	End of retention period
Contact details	Head of organisation	5 years or earlier if consent is withdrawn	End of retention period
Images taken	Head of organisation	5 years or earlier if consent is withdrawn	End of retention period
Paper Diaries	Head of organisation	3 months from the period in which its use ends.	End of retention period
Policies	Head of organisation	Until new policy has been put into place	End of retention period

Information Asset	Information Owner Asset	Retention	Trigger for Disposal
Client records including session notes, initial consultation notes and client overview form	Head of organisation	Records held until the child's 25th birthday.	End of retention period
Safeguarding records	Head of organisation	Records held until the child's 25th birthday.	End of retention period
Waiting lists	Head of organisation	Annual review period every January, old waiting list destroyed and new waiting list developed with any remaining live data transferred to new live document.	End of retention period
Worker supervision records	Head of organisation and workers supervisor	To be retained when worker is in service and until 8 years afterwards.	End of retention period
Tax returns	Head of organisation	6 years from the end of the financial period to which they pertain to.	End of retention period
Incident/Accident reports	Head of organisation	40 years from date report was closed	End of retention period
Insurance policies	Head of organisation	40 years from date policy ended.	End of retention period
Complaints	Head of organisation	2 years from complaint being resolved	End of retention period
Right to Erasure Request	Head of Organisation	8 years from request being submitted and completed.	End of retention period

Information Asset	Information Owner Asset	Retention	Trigger for Disposal
Subject Access Request	Head of organisation	8 years alongside session notes, or plus 2 years from case closure if request is made after 6 years of storing data.	End of retention period

Hard copy data will be destroyed via a cross shredding machine owned by the organisation or through the secure waste disposal services on the premises, electronic data will be permanently deleted.

Data Processing

What are the lawful basis for processing data at Nest Play Therapy?

- In relation to communicating with my clients: The individual has given clear consent for their data to be processed for the specific purpose/s detailed in the consent form stored in their personal file.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for your legitimate interests as specified in Article 9 of the GDPR;

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member

State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

This means that Nest Play Therapy does not require consent to hold your data to provide a service but does require your consent to contact you for specific purposes. Participating in the service by attending more than one appointment implies that you agree with the Terms and Conditions provided to you at the commencement of service delivery.

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. Clients wishing to understand how their own personal information is processed may choose to read the FAQs.

Reasons/purposes for processing information

Nest Play Therapy processes personal information to enable the provision of Child-Centred Play Therapy and to maintain accounts and records.

Type/classes of information processed

Nest Play Therapy processes information relevant to the above reasons/purposes. This information may include:

- personal details
- family, lifestyle and social circumstances
- education details

Nest Play Therapy also processes sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature

Nest Play Therapy processes personal information about:

- clients
- business contacts
- supervisors

Data Breach

All personal and sensitive data held by Nest Play Therapy is held securely. Electronic data stored on a computer is stored on a password protected computer, in password protected documents held on the C: Drive of the computer. This supports the ability to retrieve data in the event of faults. Hardcopy data is held securely in a locked cabinet behind a locked door.

In the case of a data breach Nest Play Therapy shall comply with the regulations set out under Article 33 of the GDPR stated below;

1. In the case of a personal data breach, the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual. Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the approximate number of data subjects concerned and the categories (e.g. sessions notes, phone numbers) and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data controller where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

6. In the event that a data breach will likely cause a risk to the rights and freedoms of client data, the data controller must communicate the nature of the breach in clear, concise and plain language, to the client/s involved, without delay.

7. If a breach occurs but the data controller has gone to appropriate lengths to protect the data held on the client (e.g. password encryption of electronic files), or if the data controller has taken subsequent action to prevent the risk (e.g. immediately blocking a mobile device) then notifying the client will not be required.

Subject Access Request

A Subject Access Requests (SAR) permits individuals to request a copy of their personal information.

A SAR must be acted upon within one month, at the most within two months, any longer and reasonable reason must be provided. There are no fees unless there is a disproportionate fee to the organisation for sending out the information. Application for SAR should be held alongside session records, unless application was made after eight years of the end of treatment. In which case the SAR will be held for a further two years after closure of SAR.

A SAR request will include information we hold about you, Nest Play Therapy will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to; and
- let you have a copy of the information in an intelligible form.

SAR requests should be put in writing to Nest Play Therapy. A response may be provided informally over the telephone with your agreement, or formally by letter or email. If any information held is noted to be incorrect an individual can request a correction be made to their own personal information. If you wish for your data to be provided to another service provider, you may also request this in writing. I may have a legal basis to continue to hold your data and will notify you of this if that is the case. Any requests should be made in writing to Nest Play Therapy.

Right to Erasure

Any person may put in a request for their personal data to be removed (the 'right to be forgotten' or the 'right to erasure'). In this instance hard copy data will be shredded using a cross shredding machine owned by the organisation or through the secure waste disposal services on the premises and any electronic data will be permanently deleted. The client will be notified of the completion. The request for deletion of data and the confirmation of completion will be held securely until eight years after the request was made. In some instances my supervisory body or insurance company may require me to lawfully hold your files until the end of their retention period. If this arises I will notify you at my earliest opportunity.

Complaints

Nest Play Therapy hopes to the meet the highest quality standards when processing personal and sensitive data. Complaints can help identify areas for improvement and therefore Nest Play Therapy would welcome you raising any concerns you have.

These Information Governance Policy documents were created to be as transparent and understandable as possible. It will not be completely exhaustive of all aspects of data collection. If you would like further information about a specific process, please contact Nest Play Therapy.

If you feel you would like to make a complaint about how your personal and sensitive data is handled by Nest Play Therapy you can contact Nest Play Therapy directly. In the event that Nest Play Therapy cannot resolve your complaint to your satisfaction you can contact the Information Commissioners Office on 0303 123 1113.

Safeguarding your privacy

In the event of my death or sudden illness, Anne Saunders will contact existing clients and archive any client files in accordance with General Data Protection Regulations.

This may mean shredding any hardcopy documents, and having any electronic documents saved on a hard drive professionally wiped or destroyed by a GDPR complaint technician.

Approved by

Debbie Moore

Nest Play Therapy

Date: 16.11.25

FAQ

What is the General Data Protection Regulations, 2018 (GDPR) and how does it affect me?

The GDPR replaces the 1998 Data Protection Act to ensure your personal and sensitive, confidential data is kept private and held securely, being processed in the way that you have agreed to. It is there to protect your rights as a consumer of a service or product that might involve your identifiable data, e.g. your name and address or whether you have a specific condition. It also covers any session records, text messages or emails we exchange. For more information your can read the policy documents accessible via your welcome information pack.

Why do you need to record this information?

I collect information about; why you are using the service, a small amount of medical information and a small amount of information about your important others, alongside brief session notes. This information enables me to provide a high quality service to you, ensuring I am equipped with the knowledge of our previous discussions prior to each session. Your contact details / address and Doctors details will only be used with your explicit consent.

I also have some third party services that collects information that cannot identify you, when you visit my website. This lets me know how many visitors visit my website, what country they are from, and how long they spend visiting my website.

What lengths are made to ensure my information is held securely?

- Hardcopy documents – Are all stored in a locked cabinet in a locked room.
- Text messages – My work phone is secured with a pin code.
- Emails – My email account requires a user name and password.
- Email attachments – Any attachments sent by email to you containing your personal information would be password protected and the password would be sent to you via text message.
- Electronic documents – Any electronic documents e.g. A letter to your GP, or an invoice, are password protected and stored on a password protected computer if they contain personal or sensitive information.

Is what we discuss kept confidential?

Everything that is spoken about during sessions are strictly confidential between you and me. To ensure I am doing my job effectively and that I have the right support, I may discuss elements of our sessions with my supervisor. During these discussions I do not disclose any details that may identify you to my supervisor, and my supervisor also adheres to the GDPR.

If there is a potential safeguarding issue, where the client or someone else might be in danger or at risk of significant harm, this must be reported to the local safeguarding board. Please see my safeguarding and child protection policy for more details.

What if I see you outside of the session?

If we see each other outside of a session I may smile but will not engage in any further conversation to ensure your confidentiality. You are welcome to share with other people about the therapy you are receiving, but I am obligated by GDPR law to ensure your confidentiality is protected. I would request that in order to ensure the success of your treatment, that you refrain from discussing your treatment with me outside of your sessions.

What about other Health and Social Care Professionals?

As I adhere to the GDPR any contact, relating to you, with other health care professionals would only be made with your signed consent. E.g. If I were to write to your GP to notify them of your treatment with me, and then notify them of the treatment ending, I would only do this if you were to sign the specific consent for this at the end of this document.

Exceptions:

In order to safeguard you and the people around you, if you were to disclose that you were going to carry out harm to yourself or someone else, then under my "Duty of Care" I am obligated by law to inform the relevant authorities. This is to support you to live well, and I would always aim to discuss this with you prior to contacting anyone.

If I was issued with a police warrant or court order for your information, by law I would also have to provide them with your information.