
THERAPEUTIC PLAY TIME

DATA PROTECTION POLICY

therapeuticplaytime.com

Therapeutic Play Time adheres to data protection and client confidentiality. Due to the nature of the work, TPT will collect certain information about individuals. Examples of these are educational settings, parents/carers/guardians, establishments, companies, organisations, services and other individuals that the service has an association with or will have in the future.

Therefore, the following policy describes how this personal data must be collected, handled and stored. This is so we can meet the Service's data protection standards and comply with the law.

Data Protection Policy of Therapeutic Play Time

What is the nature of this policy?

This data protection policy ensures that TPT Service complies with the following:

- Data protection law and good practice
- Protection of the rights of customers and partners
- How it stores and processes individuals' data
- Protection from the risks of a data breach

Data protection law

The DPA (Data Protection Act, 1998) and the GDPR (General Data Protection Regulation, effective in the UK from 25 May 2018) describes how organisations and services must collect, handle and store personal information.

As a result, data must be stored appropriately, regardless of whether it is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Law is underpinned by eight important principles. The principles state that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes

-
- Be adequate, relevant and not excessive
 - Be accurate and kept up to date
 - Not be held for any longer than necessary
 - Processed in accordance with the rights of data subjects
 - Be protected in appropriate ways
 - Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

This policy applies to Susan Andrews at Therapeutic Play Time.

It applies to all data that the Service holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ICE (in case of emergency) contact details
- Additionally, any other information relating to individuals

Data protection risks

This policy assists to protect service users from real data security risks, including:

- Breaches of confidentiality – information being given out inappropriately
- Failing to offer choice – all individuals should be free to choose how the Service applies data relating to them
- Reputational damage – It could cause great difficulty for service users if hackers successfully gained access to sensitive data

Responsibilities

has the responsibility of:

- Keeping updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related policies annually

-
- Handling data protection questions from service users covered by this policy
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
 - Performing regular checks and scans to ensure security hardware and software is operating correctly

Service guidelines

- Only Therapeutic Play Time is able to access data covered by this policy when it is required for work purposes
- Data will not be shared informally. All data will be treated as confidential and personal information
- Therapeutic Play Time will ensure all data is secure, by taking sensible precautions and adhering to the guidelines listed below:
- Strong passwords will be used and never disclosed to anyone
- Personal data will not be disclosed to unauthorised people, either within the service or externally.
- All data will be regularly reviewed and updated if it is discovered to be out of date. If any data is no longer required, it should be deleted and disposed of in the correct manner

Data storage

These rules describe how and where data should be safely stored. Any questions about storing data safely can be directed to Susan Andrews (Therapeutic Play Time), the data controller.

Paper storage: Data should be kept in a secure place where unauthorised people cannot access it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When they are not required, the paper or files should be kept in a locked drawer or filing cabinet
- Data printouts should be shredded and disposed of securely when no longer required

Electronic storage: data must be protected from unauthorised access, accidental deletion and malicious hacking attempts

- Data should be protected by strong passwords that are changed regularly and never shared with anyone

-
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services
 - Servers containing personal data should be sited in a secure location, away from general office space
 - Data should be backed up regularly. Those backups should be tested frequently, in line with the company's standard backup procedures
 - Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
 - All servers and computers containing data should be protected by approved security software and a firewall

Data Use

Personal data does not have value to Therapeutic Play Time unless the service can make use of it. However, when personal data is accessed and used, it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, the service should ensure the computer, laptop or tablet is constantly protected when left unattended
- Personal data should not be shared informally.

Data Accuracy

The law requires Therapeutic Play Time to take reasonable steps to ensure data is kept accurate and up to date.

- Data will be held in as limited places as necessary. There will not be any unnecessary additional data sets
- The service will take every opportunity to ensure data is updated. For instance, by confirming details during a call
- Therapeutic Play Time will make it easy for data subjects to update the information the Service holds about them
- Data should be updated as inaccuracies are discovered

Subject Access Requests

All individuals who are the subject of personal data held by Therapeutic Play Time are entitled to:

- Ask what information the Service holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date.

-
- Be informed how the Service is meeting its data protection obligations

(This is confirmed during Initial Parent/carer meeting)

If an individual contacts the Service requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller, suemcq@mac.com

The data controller can supply a standard request form, although individuals are not required to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Therapeutic Play Time will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

Providing information

Therapeutic Play Time aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights. (Again, this is confirmed during Initial Parent/carer meeting)

Therapeutic Play Time is legally required to be on the Register of Information Commissioners Office.