Privacy Policy Statement for CATTS Ireland

When you use CATTS you trust us with your information. This privacy policy is meant to help you understand what data we collect, why we collect it, and what we do with it. We have tried to make it as simple as possible but if you have any questions please contact us.

The Directors of CATTS assumes the function of data controller and supervises the compliance with General Data Protection Regulation (GDPR) within the business.

1 Information we collect

CATTS holds personal data as part of conducting a professional service. The data follows under the following headings: healthcare records, educational records, clinical records, general administrative records, financial records.

1.1 Healthcare records

A healthcare record refers to all information collected, processed and held both in manual and electronic formats pertaining to the service user and their care. Speech and language problems can be quite complex, and a wide range of information may be collected in order to best meet the needs of the client, and to maintain a high quality service which meets best practice requirements. In order to provide a high quality service, a range of information may be collected.

Examples of data collected and held on all current and active clients may include the following:
Contact details: Name, address, phone numbers, e-mail address,
Personal details: date of birth,
Other contacts: name and contact details of GP and any other relevant healthcare professionals involved.

For child services:
Parent/guardian details
Description of family

Educational placements.
Pre- and post-natal history: This can include information relating to mother's pregnancy, and child's birth.
Developmental data: developmental milestones, feeding history, audiology history.
Medical details: such as any relevant illnesses, medications, and relevant family history. Reports from other relevant allied health professionals such as: Audiology, Psychology, CAMHS (Child & Adolescent Mental Health Services), Occupational therapy, Physiotherapy, Ophthalmology.

For adult services:
Employment/vocational history
Mental health

1.2 Educational records

Relevant Individual Educational Plans (IEPs), progress notes from educational staff and school reports may be held.

1.3 Clinical records

Specific data in relation to communication skills may be collected and held such as assessment forms, reports, case notes, e-mails, text messages and transcripts of phone. Audio and video files may also be collected and stored.

1.4 General administrative records

CATTS may hold information regarding attendance reports and accident report forms.

1.5 Financial records

A financial record pertains to all financial information concerning the practice, e.g. invoices, receipts, information for Revenue. CATTS may hold data in relation to: on-line purchasing history, card payment transactions, receipts and invoices. Information will include name of bill payer, client name, address and record of invoices and payments made.

CATTS do not record and keep Credit Card information. Any data given for payment is processed directly via the card payment processor's own secure portal.

2 Where we get our information

Personal data will be provided by the client, or in the case of a child (under 16yrs), their parent(s)/guardian(s). This information will be collected as part of a case history form prior to, or on the date of first contact.

Information may also be provided directly from relevant third parties such as schools, medical professionals and allied health professionals, with prior consent from the parent(s)/guardian(s).

All clients are required to complete and sign either the 1 page Adult, or Child referral form which outlines your data protection rights and our privacy policy.

3 How we use the information that we collect

We use the information we collect to provide assessment and therapy as per the relevant professional guidelines, as well as to maintain the general running of the business, such as running our electronic booking system, keeping our accounts and updating you of any changes in policies or fees.

3.1 Data retention periods

The retention periods are the suggested time periods for which the records should be held based on the organisation's needs, legal and/or fiscal precedence or historical purposes. Following the retention deadline, all data will be destroyed under confidential means.

3.2 Client Records

3.2.1 Clinical Records

CATTSkeeps both physical and electronic records of clinical data in order to provide a service.

- The preferred format is X for clinical data.
- Clinical data is deleted/confidentially destroyed after 2 years from last invoiced session. (Usually post discharge).
- Video records/ voice recordings relating to client care/videoconferencing records may be recorded with consent, analysed and then destroyed. If written consent is provided to use recordings for training purposes, the client will have the option to withdraw consent at any time.

3.2.2 Financial Records

CATTS Ireland keeps electronic/paper records of financial data from those who use our services.

Section 886 of the Direct Tax Acts states that the Revenue Commissioners require records to be retained for a minimum period of six years after the completion of the transactions, acts or operations to which they relate. These requirements apply to manual and electronic records equally.

- Financial Data is kept for 6 years to adhere to Revenue guidelines.
- Financial Data (including non-payment of bills) can be given to Revenue at Revenue's request.

3.2.3 Contact Data

Contact Data is kept for 6 years to allow processing of Financial Data if required. (This may be retained for longer for safety, legal request, or child protection reasons.)

3.3 Exceptions

If under investigation or if litigation is likely, files must be held in original form indefinitely, otherwise files are held for the minimum periods set out above.

4 Information we share

We do not share personal information with companies, organisations and individuals outside CATTS unless one of the following circumstances apply:

4.1 With your consent:

We will share personal information with other relevant health care providers or educational providers when we have your written consent to do so. We require opt-in consent for the sharing of any sensitive information.

4.2 For legal reasons:

We will share personal information with companies or organisations outside of CATTS if disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process or enforceable governmental request.

- Meet the requirements of the Children First Act 2015
- To protect against harm to the rights, property or safely of CATTS, our service users or the public as required or permitted by law.

4.3 For processing by third parties/external processing

The following third parties are engaged for processing data:

Who	Type of data	Purpose
Administrative staff	Record keeping, typing, correspondence.	Updating records
Accountant	Financial	Processing financial accounts
Siteground	Contact & received files encrypted on CATTS designed bespoke CMS system.	Record keeping of client contact, financial and clinical data in encrypted database.
Microsoft	- Email & Calendaring Systems. - Attached files from main Client Management Systen	- All scheduling and correspondence through the @catts.ie domain and email. -Backup copy of main Client Management System files and notes.

5 Sharing Data

5.1 Legal requirements

CATTS is required to share data with external parties in the following circumstances:

- Compliance with local tax and audit laws.
- Compliance with child protection.
- Compliance with law enforcement.

5.2 Financial requirements

CATTS also is required to share Financial data with Chris Walshe (CJ Walshe Ltd), in order to comply with local tax laws. CATTS has obtained a copy of the CJ Walshe's own Data protection policy.

5.3 Other parties

Any transfers outside the above which contain Personal Identifying Information (PII) to third parties such as hospitals, GPs, nursing homes, are only made once the owner of the data has given express written permission by letter or email to do so.

5.4 Transfer of personal data outside the EEA

CATTS has chosen to use companies which reside and have data centres based in the EU.

Siteground – Amsterdam data centre

Microsoft – Dublin data centre.

6 How and when we obtain consent

Prior to initial assessment or consultation, a copy of the data protection policy will be provided to clients along with a client contract. A consent form will need to be signed by the client prior to commencing in the service. Copies of the signed consent forms and client contract will be given to both parties.

A consent form may also be attached onto any initial bookings via our on-line booking system. Users will be directed to read the privacy statement and to tick to agree to the terms. Services cannot be initiated without ticked consent to our set to privacy policy.

Should a client wish to withdraw their consent for data to be processed, they can do so by contacting CATTS through: data@cattsireland.com
This will send an immediate email outlining the steps you can take immediately to remove consent, as well as allowing us to follow up with you on any specific requests.

7 How we protect your data

In accordance with the General Data Protection Regulation (GDPR), we will endeavour to protect your personal data in a number of ways:

7.1 By limiting the data that we collect in the first instance

All data collected by us will be collected solely for the purposes set out at 1 above and will be collected for specified, explicit and legitimate purposes. The data will not be processed any further in a manner that is incompatible with those purposes save in the special circumstances referred to in section 5.1. Furthermore, all data collected by us will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected which include, *inter alia*, the assessment, diagnosis and treatment of speech, language and communication disorders.

7.2 By transmitting the data in certain specified circumstances only

Data will only be share and transmitted, be it on paper, electronically only as is required, and as set out in section 3.

7.3 By keeping only the data that is required,

when it is required and by limiting its accessibility to any other third parties.

7.4 By disposing of/destroying the data once the individual has ceased receiving treatment

within *2 YEARS* of the completion of this treatment apart from the special categories of personal data as set out at 1.1 above. Where data is required to be held by us for longer than the period of 2 years we will put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These may include measures such as the encryption of electronic devices, pseudonymisation of personal data, and/or safe and secure storage facilities for paper/electronic records.

7.5 By retaining the data for only as long as is required

which in this case is 2 years except for circumstances in which retention of data is required in circumstances set out at part 1.1 above or in certain specific circumstances as set out at Article 23(1) of the GDPR.

7.6 By destroying the data securely and confidentially after the period of retention has elapsed.

This could include the use of confidential shredding facilities or, if requested by the individual, the return of personal records to the individual.

7.7 By ensuring that any personal data collected and retained is both accurate and up-to-date.

You can request your therapist to update the information directly themselves, or submit a request to amend to data@cattsireland.com

8 Protecting your Rights to Data

8.1 Adult clients

Adults have the right to request data held on them as per article 15 of GDPR. A request must be made in writing. Further information regarding accessing your personal data are available in the document 'Rights of Individuals under the General Data Protection Regulation', downloadable from: www.gdprandyou.ie

8.2 Children

For children under the age of 16, data access requests are made by their guardians. When a child turns 16, then they may make a request for their personal data. However, this is subject to adherence with the Children First Act.

9 Security

CATTS, as with most providers of healthcare services is aware of the need for privacy. As such, we aim to practice privacy by design as a default approach, and only obtain and retain the information needed to provide you with the best possible service.

All persons working in, and with CATTS in a professional capacity are briefed on the proper management, storage and safekeeping of data.

All data used by CATTS including personal data may be retained in any of the following formats:

1. Electronic Data
2. Physical Files

The type of format for storing the data is decided based on the format the data exists in.

Where applicable, CATTS may convert physical files to electronic records to allow us to provide a better service to clients.

9.1 Data Security

CATTS understands that the personal data used in order to provide a service belongs to the individuals involved. The following outlines the steps which CATTS use to ensure that the data is kept safe.

9.1.1 Electronic Data

All electronic data is contained in the following systems:

[CIT]: CMS System owned by CATTS.
- This system is physically located in Netherlands.
- This system provider is aware of their requirements for GDPR compliance.
- The system has an internal administrator / Database owner. System provider personnel do not have access to CIT data.
- This system has a Live Update for security enabled.

- All persons working in CATTS have *READ/WRITE/ DELETE* access to records.
- All persons require a Log on and Password in order to access the records.
- A copy of the files are made on the users' computer when in use.
- The data controller in CATTS can remove or delete users.
- The data controller in CATTS change users passwords.

[Microsoft 365]:
- This system is physically located in Ireland.
- This system provider is aware of their requirements for GDPR compliance.
- The system has an internal administrator. System provider personnel do not have access to password data.
- This system has a Live update for security enabled.
- All persons working in CATTS have *READ/WRITE/ DELETE* access to their own emails.
- All persons working in CATTS have *READ a*ccess to their colleagues calendars.
- All persons require a Log on and Password in order to access the records.
- A copy of the files are made on the users' computer when in use.
- The data controller in CATTS can remove or delete users.
- The data controller in CATTS can force user password changes.

9.1.2 Physical Files

All physical data is located in either:

Enfield, Co. Meath.
- This system is physically located at CATTS, Enfield.
- Only CATTS have access to these records.
- These records are kept in a secured location within the building.

Ace Park, Clondalkin.
- This system is physically located at CATTS, Ace Park Clondalkin.
- Only CATTS personnel have access to these records.
- These records are kept in under lock and key within the building.

9.2 Security Policy

9.2.1 CATTS understands that requirements for electronic and physical storage may change with time and the state of the art. As such, the data controller in CATTS reviews the electronic and physical storage options available CATTS every 6 months.

9.2.2 All physical devices (including mobile phones) used by persons working in CATTS which may contain any identifiable PII are enabled with loss theft tracking and remote wipe abilities.

9.2.3 All persons working in CATTS are aware and briefed on and refresh the requirements for good data hygiene every 12 months. This briefing compliance is monitored by CATTS data controller and includes, but is not limited to:

- Awareness of client conversations in unsecure locations.
- Enabling auto-lock on devices when leaving them unattended, even within clinic locations.
- Use of non-identifiable note taking options. (initials, not names).
- The awareness of CATTS procedure should a possible data breach occur, either through malicious (theft) or accident (loss) of devices or physical files.

Date of document: 25/04/2018
Review Date: 25/04/2019