



DATA PROTECTION POLICY

for

Dyspraxia Association of Ireland trading as Dyspraxia DCD Ireland

CharityNo.1011659

Company No 2695822

Data Protection Policy

Version Date	01.02.2023
Version Number	v.5
Implementation/Approval Date	
Review Date	01.02.2024
Review Body	BOM
Policy Reference Number	

Contents

1 Summary	3
2 Data protection principles	3
3 General provisions	4
4 Lawful, fair and transparent processing	4
5 Lawful purposes	4
6 Data minimisation	5
7 Personal Data	5
8 Accuracy	5
9 Archiving / removal	6
10 Security	6
11 Request to delete Personal Identifiable Records	6
12 Breach	7
Appendix A	8
POTTS SPECIFIC: PRIVACY AND RECORD KEEPING	8
CLIENT DOCUMENTATION	8
Storage:	8
Student access to Client’s Notes/Personal Information	8
Emails	8
Progress Notes	9
Reports:	9
i. LIAISON WITH OTHER PROFESSIONALS	10
ii. DOCUMENTATION PROCESSES AND GDPR	10
iii. CONFIDENTIALITY	11
iv. RECORDING OF SESSIONS	11
v. REQUEST FOR PHOTOS/VIDEOS OF THE CLIENT FOR INTERVENTION PURPOSES:	12

Definitions

Organisation	Means Dyspraxia/DCD Ireland
GDPR	The General Data Protection Regulation.
Personal Data/Personally identifiable information/PID	Any information which are related to an identified or identifiable natural person. Also incorporates any de-identified information that by the nature of its parts may enable the person/location to be identified.
PHI/Protected Health Information	Any individually identifiable health information transmitted or maintained in a medical record paper or electronic, or designated data set that was created, disclosed, or used in the course of providing a health care service such as diagnosis, payment or treatment.
Responsible Person/s	The Chief Executive Officer (CEO) and the Data Protection Officer(DPO)
Social Media	Internet based virtual communities and networks such as websites, Facebook, Twitter, Instagram, Snapchat, TikTok etc.,
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data . Controllers make decisions about processing activities.
Data Processor	The processor or data processor is a person or organization who deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing
Requestor	An individual who on their own behalf or on the authority of another person, requests a copy of any of their personal data held by the organisation or passed on to third party contractors.
Data Subject Access Request (DSAR)	A request to the organization that gives individuals a right to access information about personal data the organization is processing about them and to exercise that right easily at reasonable intervals, in order to be aware of, and verify the lawfulness of the processing.

1 Summary

Dyspraxia/DCD Ireland is committed to protecting the privacy and personal data of our members, supporters and other stakeholders in compliance with the Data Protection Acts 1988 and 2003, as amended in 2018, and will comply with all applicable legislation including the General Data Protection Regulation (GDPR 2016/679), and the Irish Privacy and Electronic Communications Regulations 2011. The purpose of this Data Protection Policy is to ensure that a consistent approach and standard is applied by Dyspraxia/DCD Ireland in collecting, using, and managing the Personal Data that the organisation collects. This Policy explains the procedures and principles the organisation follows in collecting, managing, and using Personal Data in full compliance with applicable data protection legislation including the GDPR.

2 Data protection principles

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

3 General provisions

- This policy applies to all personal data processed by Dyspraxia/DCD
- The Dyspraxia/DCD nominated Data Protection Officer (DPO) shall take responsibility for Dyspraxia/DCD's ongoing compliance with this policy
- This policy shall be reviewed at least biannually

4 Lawful, fair and transparent processing

To ensure its processing of data is lawful, fair and transparent, Dyspraxia/DCD shall maintain a Record Management System which shall be reviewed at least annually.

Individuals have the right to access their personal data and any such Data Subject Access Requests made to Dyspraxia/DCD shall be dealt with in a timely manner

5 Lawful purposes

All data processed by Dyspraxia/DCD must be done on one of the following lawful bases:

- consent
- contract
- legal or regulatory obligation
- vital interests
- public task
- legitimate interests

All Personal Data processed by the Organisation shall be done so on the basis of opt – in consent provided directly by each individual providing data.

Consent will be obtained in written form as part of membership joining forms and renewal form. A record will be kept of each written consent.

Where information is obtained orally (by telephone or in person), the person providing Personal Data will be informed upfront that any Personal Data provided will be stored and used in accordance with this Policy.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent shall be clearly available and systems shall be in place to ensure such revocation is reflected accurately in Dyspraxia/DCD's systems.

Consent will be recorded in the notes of the call or meeting in Salesforce and or in the Record Management System.

6 Data minimisation

Dyspraxia/DCD shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7 Personal Data

In carrying out its activities Dyspraxia DCD Ireland collects certain Personal Data from members of the Organisation and from persons contacting and interacting with the Organisation. The Personal Data collected comprises personal identification information including names, email address, home address, phone number.

Dyspraxia/DCD Ireland collects and processes Personal Data in the following circumstances:

- a) Online member registration
- b) Calls made to the Dyspraxia/DCD Helpline.
- c) Email queries sent to info@dyspraxia.ie
- d) Forums, events, and workshops run by the organisation

Personal Data is collected only for the following purposes (**Purposes**):

- a) To enable the Organisation to communicate effectively with its members and other people who may require support or advice from the organisation.
- b) To allow the Organisation to collate de-identified statistical data to support its objectives of promoting awareness and understanding of Dyspraxia/DCD and in relation to obtaining support from Government bodies to further the objectives of the Organisation.
- c) To employ staff and volunteers within the Organisation.

8 Accuracy

Dyspraxia/DCD shall take all reasonable steps to ensure personal data is accurate.

Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date

9 Archiving / removal

To ensure that personal data is kept for no longer than necessary, Dyspraxia/DCD shall put in place a Data Retention policy for each area in which personal data is processed and review this process annually.

The Data Retention policy shall consider what data should/must be retained, for how long, and why.

10 Security

Dyspraxia/DCD shall ensure that personal data is stored securely using modern software and systems that are kept up-to-date. Access to personal data shall be limited to personnel who need access for legitimate purposes and appropriate security shall be in place to avoid unauthorised sharing of information.

When personal data is deleted this will be done safely such that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions shall be in place.

11 Request to delete Personal Identifiable Records

Under GDPR legislation (Article 17), any person has the right to request that any PID is destroyed under 'Right to be Forgotten' unless there is a legal obligation to keep the data or reasons of public interest.

A person has the right to have their data erased, without undue delay, by the data controller, if one of the following grounds applies:

1. Where your personal data are no longer necessary in relation to the purpose for which it was collected or processed.
2. Where you withdraw your consent to the processing and there is no other lawful basis for processing the data.
3. Where you object to the processing and there are no overriding legitimate grounds for continuing the processing (see point 6 below).
4. Where you object to the processing and your personal data are being processed for direct marketing purposes (see point 6 below).
5. Where your personal data have been unlawfully processed.
6. Where your personal data must be erased in order to comply with a legal obligation.
7. Where your personal data have been collected in relation to the offer of information society services (e.g. social media) to a child.

Should such a request be made it must be by letter or email and addressed to the Data Protection Officer (DPO). The following procedure should take place:

- The CEO should be made aware of the request to delete personal information.
- The request for data deletion should be recorded and stored in a central location. At this point, the requestee should be informed that the data deletion process has begun.
- All personal data should be identified, all backup locations/copies should be noted, and if there is any instance of a 3rd party (data sub-controller or joint controller) having access to the personal data, those parties must be informed of the data deletion request, and the requestor should be informed of who those 3rd parties are.
- The DPO and CEO should make a final determination on whether there is any valid reason to hold on to the personal data in question. Should there not be, the data should be destroyed, and the requestor should be notified in writing that the action has occurred.
 - If there is a valid reason that the personal data should be maintained, the requestor should be notified of the reason/s in writing, and the data should be maintained.
- The whole process should be logged in a central location, and the date that the data is deleted should be recorded. Other important log notes:
 - Each communication (internal within Dyspraxia DCD and with the requestee) should be logged in the file
 - The documentation to the process for data removal
 - Verification that the data was removed
 - Final notification to the requestee that the data was removed.

12 Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Dyspraxia/DCD shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Data Protection Commission within 72 hours of discovery of a breach.

Appendix A

POTTS¹ SPECIFIC: PRIVACY AND RECORD KEEPING

CLIENT DOCUMENTATION

Storage - All POTTS client documentation and reports containing sensitive client information in relation to medical history, clinical observations, or clinical needs, will require to be stored on Salesforce in the POTTS specific folder, which only professionals and student therapists working with the POTTS programme will have access to. Some documentation may be developed using the students OneDrive (online encrypted cloud-based storage) and should be uploaded to sales force immediately upon completion.

Student access to Client's Notes/Personal Information - Students will be given temporary access to the POTTS client files which are held on Salesforce (CRM system) on commencing placement. Access to Salesforce will be removed on the student's last day of placement.

Emails

- a) A password, specific to each client, will be generated at the start of each placement. The lead therapist and the therapy team will have access to the password assigned to each client participating in the programme.
- b) Where it is necessary for the POTTS lead therapist/therapy team to send reports and documentation containing sensitive client information in relation to medical history, clinical observations or clinical needs, the sender will be required to password protect each document or file prior to it being sent via email, where feasible.
- c) During student placements, the practice educator/team of practice educators (Supervising Occupational Therapists) and student occupational therapist team will have access to the password assigned to each client participating in the programme.
- d) At the beginning of each therapeutic interaction the parents of clients or the client themselves (in the case they are over 18) will be contacted directly via phone call by the occupational therapist working with the client. During this phone call, the occupational therapist will provide the parent/individual with a unique client-specific password which will be required to access personal reports and documentation sent by the occupational therapist.
- e) At the beginning of each placement, the parents of clients or the client themselves (in the case they are over 18) will be contacted directly via phone call by the occupational

¹ POTTS – Partnering in Occupational Telehealth Services, a clinical assessment and follow on supports programme operated by Dyspraxia/DCD Ireland

- therapy student who is working with the client. During this phone call, the student will provide the client with a unique client-specific password which will be required to access all future personal reports and documentation sent by the occupational therapy student.
- f) This client-specific password will then be used to password-protect reports and other documentation deemed sensitive being sent via email to the client. This will be completed by the occupational therapist/ Occupational therapy student prior to the sending of the report/document.
 - g) If the parents request to be sent the password again. A second phone call will be arranged with the occupational therapist or occupational therapy student working with the family, whereby the password will be shared via phone call.
 - h) In the case that a client/family may have difficulty accessing encrypted emails, their written permission to send information via unencrypted mail must be consented to in writing. Once this permission has been received you can proceed with communication without encryption.
 - i) All student email correspondence should be cut and pasted across to a word document, ensuring that the email address of the recipient/sender and the date & time of the correspondence is documented. Alternatively, screenshots of all emails can be taken. These should be documented for the duration of the placement, with all screenshots deleted after emailing. Educators should sign off on all emails on a weekly basis and, at the placement end, students will PDF this document and transfer it to the client file. It is the responsibility of the student to ensure e-mails are reviewed and signed by both the student and educator and deleted upon the completion of the placement.

Progress Notes

- a) Progress notes must be completed within 24 hours of the intervention/ encounter. Once signed by the therapist the note should be saved to word or PDF format and moved to the client file.
- b) Student Progress notes: Progress notes must be completed within 24 hours of the intervention/ encounter. Once signed by both the student and educator the note should be saved to PDF format and moved to the client file.

Reports

- a) All handover/discharge reports should be completed in the timeframe dictated by the therapist. This will then be signed by the therapist and then be saved in the client in PDF format.
- b) All student-led handover/discharge reports should be completed in the timeframe dictated by the educator team. Drafts will be reviewed by the practice educator and feedback is given. A new report should be started and all feedback amalgamated. This will then be counter-signed by the practice educator and should then be saved in the client's file in PDF format.
- c) Home-Programmes: If required, home programmes should be developed and forwarded onto the family with the discharge report and any resources and power-points, once signed (and counter signed in the case of student therapists) and converted to PDF.
- d) Onward referrals: Copies of all onward referrals must be kept within the client file and must be checked and signed before a PDF version is forwarded on to the relevant agency via encrypted email. Clients/ families should also receive a copy of the referral for their personal records. Clients and families should give informed explicit consent to onward referrals prior to making these.
- e) Records provided to the client/family: Unless the client/family specifically requests copies of all documentation kept, only the following records should be forwarded to the person/family via encrypted email (as feasible):
 - a. PDF version of the assessment/discharge report
 - b. PDF version of the home programme
 - c. PDF copy of any onward referrals

LIAISON WITH OTHER PROFESSIONALS

Informed and explicit consent will be obtained from clients prior to liaising with other professionals regarding their case.

DOCUMENTATION PROCESSES AND GDPR

- a) OneDrive
 - a. All student documentation will be completed on OneDrive. Each student will have a personal folder for draft clinical records, supervision agendas/minutes and all other placement documentation including the hours sheet, CBF: OT and induction checklist.
- b) Management of Clinical files
 - a. Once clinical documentation is completed it should be uploaded to the client/family's Salesforce folder
- c) Management of personal files
- d) Within one drive students should create sub-folders within their personal folder entitled:

- a. Notes for review
 - b. Historical drafts
 - c. Placement documentation,
 - d. Supervision Records.
- e) All draft notes/minutes/reflections/session plans should be placed within the review folder, to be reviewed by a member of the practice education team. Once counter-signed, they should be saved in PDF format and transferred to the relevant long-term storage folder.
- f) Email contact with clients/families: All contact with clients/families should preferably be through encrypted email but if using unencrypted mail, ensure that permission is given for same in written/email format.
- g) Deletion of Data Form: At the end of the placement, students will be required to submit a Deletion of Data form to their practice educator, which must be counter-signed by one of the educator team. This will be a statement that students have disposed of all hand-written notes in a confidential manner, deleted all client-related emails and ensured that no draft notes have been kept on a home device. It should be noted that all documentation should be completed within OneDrive to avoid the latter.

CONFIDENTIALITY

All staff working with the POTTS programme will be required to sign a Confidentiality Agreement. When working with clients it is also imperative that staff ensure a private space, in which client sessions cannot be seen/overheard by others in the vicinity. Students will be required to sign a Confidentiality Agreement. When working with clients it is also imperative that students ensure a private space, in which client sessions cannot be seen/overheard by others in the vicinity. Please note that students should also maintain the confidentiality of their peers within the placement setting.

RECORDING OF SESSIONS

Client sessions are not recorded using video or audio recording devices, without specific consent gained prior to sessions, in order to protect the privacy of clients.

REQUEST FOR PHOTOS/VIDEOS OF THE CLIENT FOR INTERVENTION PURPOSES

Clients and/or families may be requested to provide video footage of the client undertaking a specific ADL task or to provide additional environmental information. However, the purpose of this must be made clear to the client/family, it must be supportive to the client intervention and the retention period that the video will be kept must be stated to the client/family before it is provided. Consent to record must be documented prior to recording. The video must be stored only online and deleted after analysis is completed and the family informed of its deletion.

