DATA RETENTION POLICY

(records retention, archiving and disposal)

for

Dyspraxia Association of Ireland trading as Dyspraxia DCD Ireland

Charity No.1011659 Company No 269582

Data Protection Policy

Version Date	March 2022
Version Number	V.6
Implementation/Approval Date	
Review Date	March 2024
Review Body	
Policy Reference Number	

Contents Page

Definitions

Organisation	means Dyspraxia/DCD Ireland.
GDPR	means the General Data Protection Regulation.
Personal Data/Personally identifiable information/PII	means 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.
Responsible Person/s	means 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.

1.0 Summary

This document outlines the process that should be followed in identifying the records retention, archiving and disposal processes in Dyspraxia/DCD Ireland. This provides assurance that the organisation is GDPR compliant and meets its legal responsibilities in relation to how records and information are recorded, stored, archived and ultimately destroyed in compliance with GDPR and Data Protection Acts 1988-2018, and within specific timelines. External assurance on retention, archiving and disposal processes in Dyspraxia/DCD Ireland in areas requiring legal or technical expertise will be sought as appropriate.

2.0 Scope

This policy covers all records/information in paper based and electronic format, with the exceptions listed below. These guidelines do not apply to situations outside of the control of Dyspraxia/DCD:

- Social media – deemed to be a "transient" record which carries an automated retention period, according to social media platform i.e. Twitter, Facebook
- Records or parts of records which are subject to any known litigation
- Child Protection proceedings or Freedom of Information requests or appeals
- Subject Access Requests (SAR)

3.0 Duties and Responsibilities

All staff are responsible for any records they create, receive and use and are responsible for adhering to the policies and procedures of Dyspraxia/DCD in relation to records management.

The Chief Executive Officer (CEO) has overall responsibility for records management within Dyspraxia/DCD. As the accountable officer and in acting as the Data Protection Officer (DPO) (he/she) is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key in ensuring appropriate, accurate information is available as required for legitimate purposes.

4.0 Storage of Records

General principles

- All records, whether electronic/paper and or confidential or public access must be stored in an easily accessible filing system, in a format appropriate to the record and with its own storage solution.
- Records that are deemed to be confidential in nature should be marked as such in the footer of each page. This includes PII, PHI, employee records, payroll, one to one client communications and internal communications.
- Conditions should be appropriate for the storage of records i.e. stored with a password and backed up to prevent data loss. Physical records should be protected against fire, flood and theft, with filing and lighting systems compliant with health and safety requirements, and kept in a clean and tidy condition.
- Movement of paper records into and out of formal filing storage must be tracked and clearly detailed on local inventories held by the service on each occasion that the file is moved. This should include the access and return dates, taker's name, contact details, signature, and reason.
- Two years of inactive paper records should be kept at an identified secure location within the organisation if capacity allows. Should capacity not exist, these documents should either be electronically archived with physical copies destroyed, or shredded after a period of twelve months.
- Older paper records should be electronically archived and stored in a secure electronic format for a period of three years. The physical copies should be destroyed. After twelve months, all personal data should be deleted in compliance with relevant GDPR legislation, unless there is a valid reason for keeping them.

5.0 Confidential or Personally Identifiable Records

All records containing personal identifiable information (PII) should be kept in a safe and secure database, additionally confidential paper records must be stored in a secure location (i.e. in a locked cupboard or filing cabinet in a room which is kept locked at all times when not in use).

Access to these records must be controlled and restricted to designated staff to maintain security of information.

All digital records must be password protected (with a non-widely used password) and only designated staff should be able to access for legitimate purposes.

6.0 Procedure for archiving paper records

- Only records with the same review date should be stored in the same box. This is to simplify review and facilitate easy destruction. The review date is calculated from the date of the last entry in the record. Administrative records from different years but with the same review date may therefore be stored together.
- Files should be 'weeded' or "culled" before archiving. This means removing documents which have no archival value (e.g. contacts lists, room-booking details in meeting papers, duplicates).
- Copies of records already held elsewhere (e.g. invoices) should not be archived.
- Signed and/or master copies of meeting records should be archived by the person responsible for managing those meetings. All other copies should be shredded.
- Copies of information already in the public domain e.g. internet downloads and printed published documents must not be archived and should be destroyed.

7.0 Archive Year

Records should be archived throughout the calendar year as they become inactive; and reviewed on an annual basis.

8.0 Request to delete Personal Identifiable Records

Under GDPR legislation (Article 17), any person has the right to request that any PII 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.

9.0 Procedure for review and destruction of records

Records stored on Dyspraxia/DCD premises must be reviewed at least annually, usually in January or April, to identify those records whose retention period has expired. The Data Protection Officer (DPO) or CEO should authorize disposal.

Records must either be destroyed on site or arrangements made with an approved contractor to carry out this task. An appropriately detailed certificate of destruction must be obtained. This must be kept indefinitely.

Destruction of confidential records must be secure and complete. Records must therefore be destroyed by shredding, combustion or pulping.

The following should be recorded: a list of the records destroyed, when this took place, the name of the person who authorised destruction, who carried out the process and the reason for destruction.

If a record is inappropriately destroyed (e.g. a record which is subject to a request under the Freedom of Information or Data Protection Acts) the DPO must advise the CEO and carry out an investigation. Inappropriate destruction may lead to disciplinary action being taken.