Records Retention and Destruction Policy

Ref: IC013, v1

June 2024

An Bord Um Chúnamh Dlíthiúil
Legal Aid Board
Providing access to justice since 1979

Policy and Procedure Document Summary

Document Governance and Management	
Document Name	Records Retention and Destruction Policy
Current Version	v1
Document Reference Number	IC013
Date Effective From	24th June 2024
Date Set for Next Review	23rd June 2026
Commissioning Directorate	Information & Communications Directorate
Commissioning Unit	Knowledge & Information
Document Owner (Director)	Gareth Clifford
Document Author	Dr. Brian Moss
Document Approver (Person or Group)	Executive Management Team
Note: Formal review may occur sooner if new legislative/regulatory or emerging issues/research/technology/audit etc. dictates sooner.	

Version Control				
Version No.	**Date Reviewed**	**Description of Change**	**Author**	**Approved by**
1	14/05/2024	Full Review	Brian Moss	Gareth Clifford

1. Purpose

The purpose of this Records Retention and Destruction Policy is to explain how the Board manages, retains and erases personal data gathered and used for carrying out its statutory role.

2. Scope

This policy applies to all personal data records collected by the Board from service users, private practitioners, staff, and service providers in hard or soft-copy/ electronic format. The Board uses these data to undertake its legal advice and consultation, mediation, and corporate service functions and collaborate with other public bodies and their agents where necessary.

3. Target Audience

This policy is intended for Board staff and service providers and clients to the Board. A copy of this policy is available on the Board website www.legalaidboard.ie.

4. Definitions

Deletion: the placing of data beyond use, if not possible to delete or erase all traces.

Record: any item containing personal data, whether in hard or soft/ digital copy format created or received from a client, staff member or other party or information created or received in the course of the Board conducting its business.

Technologies: encompass the computer network, system, domains, internet, email, instant messaging, video call platforms, and devices including but not restricted to printers, photocopiers, scanners, fax, telephones, mobile telephones, applications, CCTV, USBs, and postal services that the Board uses and makes available to staff through which to undertake its work.

5. Roles and Responsibilities

Staff of the Legal Aid Board: all are individually responsible for reading, understanding, and complying with obligations of the GDPR, the Data Protection Act 2018, set out in this policy, and in all Board data policies in their daily work. All policies are available on www.legalaidboard.ie. Staff are also individually responsible for engaging with data protection training provided by the Board.

Data Owners: are senior managers (e.g. Directors, Managing Solicitors and Managing Mediators) in each functional area responsible for the records and data processed in or on behalf of their area. Data Owners have overall operational responsibility for records management, retention, and destruction implementation and compliance including determining processing tasks, assigning staff to undertake this work, facilitating staff training, ensuring standard and local procedures are in place and compliant with GDPR.

Data Protection section: advises on and monitors compliance with data protection legislation, taking timely action and making recommendations to improve the Board's performance where needed. The section should be consulted for guidance on this policy by a local business unit manager where necessary. The Data Protection section acts as the main contact point for the Data Protection Commission, the Irish supervisory authority on data protection on all matters relating to this policy.

6. Management and Retention of Records

The general principle to the Board's data retention approach is that it will retain records containing personal data only for as long as is necessary to undertake its statutory role.

It should also be noted that the Board utilises a range of technical and organisational security and audit measures in place to limit the access to and loss, theft, alteration, or misuse of personal data. These range from physical safeguards in the workplace to digital measures. Board staff receive access only to such personal data as are necessary to complete their work. They are also required to respect all personal data with which they come into contact and to keep it confidential. The Board undertakes an assessment of all third parties to whom it plans to transfer/ receive personal data.

Where a breach arises, the Board undertakes an assessment of whether to inform the Data Protection Commission and the person whose data are at issue, in compliance with GDPR.

6.1 Records Management

A comprehensive records management approach entails the creation, classification, storage, business continuity planning, and destruction of information. Across all stages the Board aims to factor in accessibility, privacy, authenticity, and security of the records it processes.

To realise the above, the following should be adhered to by all staff and Data Owners:

1. All records created in the course of their work by Board employees are the property of the Board.
2. All new records/ files naming should be consistent and logical.
3. All records collected should only be that information necessary for the purpose.
4. All records should be accurate and complete at the current point in time.
5. All records are created and retained with a view to minimising space and cost use.
6. Active cases are kept within easy reach of staff within local units, whether in hard or soft copy format.
7. All records are stored securely in local business units in a manner that respects health and safety requirements.
8. Access to records is restricted for designated staff only.
9. Any records shared between Directorates/ Units must have an identified Controller. This Controller must lead on determining how records are created, managed, stored, and destroyed when no longer needed.
10. Adopted Board guidance, including in Administrative Procedures Handbooks, should reflect GDPR principles and be reflected in turn in daily procedures.
11. Hard copy versions of closed records (e.g. cases) are kept off-site in a secure arrangement.

6.2 Records Retention

- Retention is the period of time for which records are kept. The Board keeps record only for as long is necessary to carry out its functions in relation to legal aid, mediation, and associated corporate services.
- The retention of different record types across the Board is set out in Appendix 1. A retention period for a Board record commences from the start of the next calendar year that follows the last entry in any record (i.e. file, transaction matter, HR issue, etc.)
- Each record type is owned by a Data Owner. Each Data Owner must determine and document for the Data Protection section any record retention period that differs from the retention periods set down in Appendix 1.

- Additionally, all staff must return records in their possession at the end of a designated task, or before leaving Board employment.

7. Destruction of Records

- When the retention period for any record expires as set out in Appendix 1, the Board deletes it in a secure manner with all erasure processes certified to recognised standards. Any record due for deletion should be checked to ensure there is no further action due on the item (e.g. a review of a file). All business units should follow adopted Directorate-level guidance for their area on the handling and destruction of records.
- Where an external company is used to destroy Board records, they should be required to sign an undertaking to comply with GDPR and confidentiality requirements and to provide the Board with certification of record destruction or disposal. This applies to all forms of hard copy, soft copy and magnetic and optical media and all technologies the Board uses in its work.
- A local business unit should maintain a register of all records destroyed, reflecting the compliance trail form in Appendix 2.
- All records identified for destruction should be destroyed within a reasonable timeframe following the end of the retention period.

8. Contact details

The Board's Data Protection section and Data Protection Officer can be contacted at the details below. These are also published on the Board's website www.legalaidboard.ie

Data Protection Officer
Legal Aid Board
Quay Street,
Cahirciveen,
Co. Kerry
V23 RD36

Phone: (066) 947 1000
Email: dataprotection@legalaidboard.ie

9. Making a complaint

A person dissatisfied with the Board's response to matters relating to its Records Retention and Destruction Policy may then submit a complaint as follows:

Data Protection Commission
21 Fitzwilliam Square,
Dublin 2.
D02 RD28
Ireland

Phone: 01 765 0100

Email: info@dataprotection.ie
Web: www.dataprotection.ie

10. Monitoring, Enforcement, and Alteration

Compliance with this policy will be monitored by the Data Protection section and the Executive Management Team members reporting to the Board Audit and Risk Committee.

The Board reserves the right to take action it deems appropriate where individuals breach this policy. Board staff who breach this policy may be subject to disciplinary action. The Board reserves the right to remedy a breach of this policy by contractors, sub-contractors and commercial service providers via contracts in existence with them.

The Board will amend this policy regularly but may amend this policy at any time to take account of business, legislative, or organisational changes.

Any changes to the policy will be notified on the Board website.

Appendix 1 Records Retention Schedule

Data Owner	Record type	i) Format ii) Location	Retention Period
Legal Services	Applications for Legal Aid	i) Hard copy and digital ii) Offices, case tracking system, and off-site storage	Unsuccessful applications- 1 year Conveyancing - 12 years All other matters- 7 years
Family Mediation Services	Administration	i) Hard copy and digital ii) Offices, case tracking system, and off-site storage	7 years
Legal Services	Assisted decision-making	i) Hard copy and digital ii) Offices and case tracking system	20 years or 8 years if after death
Finance	Pension data	i) Hard copy and digital ii) Offices and internal systems	7 years after death of individual
Finance	Taxation, pay awards, increments	i) Hard copy and digital ii) Offices and internal systems	Indefinite
Various Directorates	All else (Finance, Human Resources, Research, etc.)	i) Hard copy and digital ii) Offices and controlled databases (e.g. Agresso, Sage)	7 years

Appendix 2 Destruction and Deletion Compliance Form

The Administrative Procedures Handbooks (page 9-10 of Civil Ops; and 5-3 of FMS) reference a disposal form/ register. They also mention retention of a spreadsheet capturing client name, reference number, the date of destruction and in the case of FMS, the date of closure.

Each local unit must therefore maintain a form along the following lines, capturing data in relation to a Board record that is to be destroyed or deleted. This applies to all client files and corporate files (e.g. finance, HR, etc.). A file is understood as comprising a complete folder of materials on one process (e.g. a procurement order, a legal aid case, an application for employment).

Destruction Compliance Form complete each row where appropriate	
File reference	
Directorate and Unit/ Office	
Client Name or Practitioner Name or Company Name	
Client or Practitioner or Company address	
Client date of birth	
Date of first contact/ opening	
Date of last contact/ closure	
File storage location at point of destruction	Local office ☐ Email ☐ Database ☐
File format	Hard copy ☐ Digital/ soft copy ☐
Date destroyed	DD/MM/YYYY
Number of items	
Destruction Method	Confidentiality bin ☐ Home shredding ☐ Digital destruction ☐ Other (specify) _____ ☐
Supervising staff member name	
Supervising staff member signature	