

Data Classification Policy

Ref: IC015, v2

September 2025



**An Bord Um
Chúnamh Dílthiúil**
Legal Aid Board

Providing access to justice since 1979

Policy and Procedure Document Summary

Document Governance and Management	
Document Name	Data Classification Policy
Current Version	V2
Document Reference Number	IC015
Date Effective From	12 September 2025
Date Effective Until	11 September 2027
Commissioning Directorate	Information & Communications Directorate
Commissioning Unit	Knowledge & Information
Document Owner (Director)	Tomás Keane
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	27/11/2024	Full Review	Brian Moss	Gareth Clifford
2	12/09/2025	Full Review	Dr. Ellen Ganly	Dr. Brian Moss



1. Purpose

The purpose of this Data Classification Policy is to explain how the Board decides the organisation, retention, release, and erasure of data in the course of its work.

2. Scope

This policy applies to all personal data collected by the Board from or relating to service users, private practitioners, staff, and service providers in hard or soft-copy/electronic format on any of the Board's technologies and those provided by contractors to the Board. It also applies to all data created by the Board in the course of its work. The Board uses these data to undertake its legal advice and consultation, mediation, and corporate service functions and to collaborate with other public bodies and their agents where necessary.

3. Target Audience

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

4. Definitions

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 Controller: the Board is the controller of all personal data it collects. The Board, through the CEO, sets the requirements for all processing of data in line with GDPR and these must be followed by data owners and staff.

Data Owners: are senior managers (e.g. Directors, Managing Solicitors and Managing Mediators) in each functional area with operational responsibility for records management implementation and compliance in or on behalf of their area. This responsibility includes classification of data under their delegated control.

IT Unit: is responsible for setting controls and ensuring these remain fit for purpose.

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. Data Classification

Data classification is how data are graded to reflect their content and the impact that a breach/ loss would create.

The Board hosts different types of data at any point in time. These are:

- Client data;
- HR data about current and past staff, including pay, pensions, qualifications, health status;
- Financial data about Board expenditure and likely commercially sensitive details from contractors; and
- Research data, obtained from clients, staff, or the general public.

It is the Board's general principle not to identify one set of data as more important than another. Board staff must bear this in mind in the course of undertaking any duties in a Board office, in remote working at the site of another organisation (e.g. court building), or blended working between their home and LAB office. Certain LAB staff are allowed to remove Board files for remote working but no staff may remove any Board documents/ files for working on them from home, i.e. under blended working arrangements. These points are clarified in the Board's Access Control Policy, available at www.legalaidboard.ie.

The Board classifies its data according to the sensitive nature and privacy of their contents and the impact of any breach of those data. Data Owners within the Board are responsible for determining on an ongoing basis into which of the following categories any of the materials under their management fall:

- **Public** (material that is already or intended to be available to the public, e.g. web content, Board announcements, application forms, qualifying criteria for Board services);
- **Internal** (items intended for staff and contractors, e.g. manuals, policies, phone directories); and
- **Confidential** (information carrying details of a personal or commercial interest and value, e.g. contract values, staff records).

The default position within the Legal Aid Board is that all data are confidential. This means that any intended release to commercial contractors or the public should be considered before any transmission/ publication. Where a business unit decides to alter the status of data it holds, the Data Owner should record this as per the Data Retention Policy.

In deciding that a category other than 'Confidential' should apply to any data, a Data Owner within the Board must consider the possibility of data being unexpectedly disclosed at any point in time and the impact of such a release. The Board categorises the impact of any unexpected release of data concerning clients, operations, assets, staff, contractors, or others in the following ways:

Low impact- limited adverse effect such as over a short-term, causing little harm

Moderate impact- some adverse effect over the medium-term, causing some harm

High impact- severe adverse effect over a long-term, causing serious harm

Any unexpected disclosure would also be deemed a data breach and should be reported to the Data Protection Officer immediately, who will determine the impact/risk level of the breach.

7. Classification Actions



- All data collected and created by the Board and its staff must be given the initial default classification of confidential until indicated otherwise by a Data Owner.
- Data Owners are responsible for maintaining an overview of file classification under their management, keeping the classification under review (i.e. to move it to/ from Public, Internal, or Confidential status).
- In deciding the classification, at all times a Data Owner should consider the possibility of a breach, the impact of a breach, and the organisation's tolerance for a breach occurring in relation to data they manage.
- Data Owners are responsible for ensuring that all access, processing, and retention activities by staff under their management are in line with the Board's other data protection policies.
- Data Owners must ensure that their staff are made aware of the requirements under this policy.
- All staff should ascertain the status of material that they are asked to work on at the outset of a task.
- All LAB devices should be locked when not in use and not visible to persons outside LAB employment or not having access entitlements to the data.
- No internal or confidential Legal Aid Board material should be or viewed or saved on a personal device.
- Printing/ scanning/ photocopying of confidential material should be limited at all times.
- Confidential information should not be transmitted by text message unless prior consent has been secured. Even then data should be kept to a minimum.
- The discussion of personal information should only be done within a private work setting, avoiding public/ open areas.
- Where confidential printed material must be sent by post it should be marked as 'Private and Confidential', be sent to the correct address, and include a return address.
- Where confidential digital material (e.g. encrypted USBs) must be sent by post it should be marked as 'Private and Confidential', be encrypted, be sent to the correct address, and include a return address.
- Where confidential material must be sent by email, it should be sent by Secure email, be sent to the correct email address, and include the sender's details.

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
48/49 North Brunswick Street,
Smithfield,
Dublin 7,
D07 PE0C.

Telephone: 01 6469 764
Email: dataprotection@legalaidboard.ie

9. Making a complaint



A person dissatisfied with the Board's response to matters relating to its Data Classification 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, Risk, and Finance 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.

