Data Encryption Policy

Ref: IC017, v1

November 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	Data Encryption Policy
Current Version	v1
Document Reference Number	IC017
Date Effective From	27th November 2024
Date Effective Until	26th November 2025
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	27/11/2024	Full Review	Brian Moss	Gareth Clifford

1. Purpose

This Data Encryption Policy is the Legal Aid Board's statement governing how staff within the Legal Aid Board should keep secure data that they use or transmit to external parties in the course of undertaking their duties. Protection of the data through encryption is essential to the Legal Aid Board maintaining a GDPR-compliant workplace. This Policy ties in with the Board's Data Access Policy and Access Control Policy.

2. Scope

This policy applies to all Board staff, to all on-site, remote, or blended working arrangements and to all data held by the Board in hard or soft/ digital formats on managed ICT services operated by the Board.

The policy should be read in conjunction with all Board data protection policies. All Board data policies are available at www.legalaidboard.ie.

3. Roles and Responsibilities

IT Unit: maintains all of the Board technologies, devices and all managed databases / systems. Where approved by the EMT, the IT Unit is responsible for ensuring that all technological measures remain fit for purpose, offering the protections expected under GDPR, to minimise risk to the Board and to maintain the Board's standing. The IT Unit is therefore responsible for implementing encryption on Board-issued devices and systems.

Executive Management Team and Directors: The Executive Management Team approves all GDPR policies and business developments for the daily functioning of the Legal Aid Board. The EMT is therefore responsible for promoting compliance with this policy across Directorates.

Local Managers: have responsibility for ensuring compliance with GDPR in the teams that report to them. As data owners, they must ensure data their Unit owns are encrypted or otherwise protected in line with GDPR expectations and adopted Legal Aid Board standards. Where wider Directorate guidance applies, a local manager must ensure that procedures within their Unit meet those requirements.

Staff of the Legal Aid Board: all are individually responsible for reading, understanding, and complying with obligations of the GDPR and 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. Individually, staff are responsible for engaging with data protection training provided by the Board to inform themselves of data protection legislation and good practice.

All staff should consult the Data Protection section if in doubt about any aspect of this policy or aspect of their work where Board data are concerned.

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. Working with the IT Unit, the Data Protection section will look to ensure this Policy remains adequate, relevant, and practical for the Legal Aid Board over time.

4. Definitions

Board Staff: for the purpose of this policy, Board staff are understood as those directly employed or contracted to undertake a service on the Board's behalf, Board members and Executive, and those given access to Board data to do this.

Data: these are personal information as defined in other Legal Aid Board Data Protection policies as well as information and details, considerations, and decisions relating to procedures, applications, and contracts already taken, in place, or under consideration by the Legal Aid Board connected to its cases and to its financial, staffing, estates, and other business.

Encryption: the securing of data by its encoding (scrambling) to prevent access by persons not authorised to view their contents. Encryption protections are reversed by those given the necessary access key/credentials, enabling them to view the data legitimately.

5. Data Encryption Policy

The data encryption requirements on all staff are set out below.

- The IT Unit will determine and implement the most appropriate encryption standard for Legal Aid Board networks/drives/systems/website maintenance/mobile devices and media. A business Unit must adhere to the IT Unit decision regarding the method of encryption/protection to be used.
- All data must be encrypted or otherwise protected when stored, in use, or when transmitted across or out of the Legal Aid Board (e.g. by email or ShareFile).
- Unit managers are reponsible for determining on an ongoing basis what data require encryption before being trasferred across or outside the Legal Aid Board. It is the responsibility of staff to be aware of their local Unit requirements in this regard.
- All keys/credentials needed to sign in to Legal Aid Board data/platforms/software/logs/mobile devices should be kept secure and separate from the data they hold.
- No mobile storage devices (e.g. USBs) should be used to secure LAB data except with the prior authorisation of the IT Unit. The IT Unit decision to allow/decline any such requests will be final. The IT will provide all such storage devices.
- All keys/credentials for Legal Aid Board systems/platforms/software/mobile devices/mobile storage devices must comply with IT Unit directions.
- A mobile storage device containing Legal Aid Board data should only be used as a temporary measure. Any data transferred by means of a mobile storage device should be moved to a secure/protected system upon receipt.

Destruction of the transferred data on a mobile device must be confirmed by the recipient to the Legal Aid Board staff member who transferred the data.

- Where a mobile storage device is used to hold/transfer data, copies of the key needed to decrypt the data should be recorded in a file accessible to necessary Unit staff. The key should not be saved in the file/drive of just one staff member in a Unit.
- Where a key/credential needs to be sent to an external party in order to access Legal Aid Board data, this should be sent by a media form different to how the data were sent (e.g. if data were sent by secure email, send the key via SMS/MMS, letter, or phone call.)
- Encrypted data and any associated key/credential should only be sent to a known, identifiable third party individual (e.g. John Brown at BigPaper Inc.), never just to a third party organisation (e.g. Sales Unit at BigPaper Inc.).
- Only IT Unit-issued or approved devices (e.g. laptops, mobile phones, etc.) should be used in the course of undertaking Legal Aid Board work.
- All IT Unit-issued devices (e.g. laptops, mobile phones, etc.) must have encryption (i.e. "full-disk" or "whole disk" encryption) in place before staff use. If a device is not encrypted, a staff member becoming aware of this must inform the IT Unit as soon as possible and the device not used further until the situation is remedied.
- If a Legal Aid Board staff member becomes aware that encryption for data is not in place or with good reason believes that encryption should be in place for a business process within the Legal Aid Board, they should raise this with their line manager at the earliest opportunity.
- Where a staff member becomes aware of any breach of this policy they must report it to their line manager at the earliest opportunity.
- All business Unit managers (e.g. Managing Solicitors, Managing Mediators, Assistant Directors or equivalent) are responsible for ensuring that data encryption or other protections are in place across their Units.
- The Legal Aid Board Data Classification Policy defines data types in use. All data classified as 'Confidential' or above must be encrypted at rest and when in transit.
- All Legal Aid Board data, including those classified as 'Public', should be encypted in order to protect its integrity.
- Where any Legal Aid Board data are to be stored in a cloud-based service, either the data should be encrypted or confirmation must be secured from the IT Unit regarding the encryption methods and access controls the service offers. It is the role of the local manager to confirm that one of these is in place. The IT Unit and Data Protection section will keep all cloud-based controls and protections under review as necessary.
- Where data are passed to a third party (e.g. under a joint controller, sharing, processor or other arrangement), any agreement governing the transfer must ensure that the external party has encryption or other appropriate protection in place for the data.
- Legal entitlements in other jurisdictions enable public authorities to access encrypted data carried by a person. As a consequence, to protect Legal Aid Board data, no confidential data should be brought abroad by any Legal Aid Board staff member.

6. 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

7. Making a Complaint

A person dissatisfied with the Board's response to matters relating to its Data Encryption 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

8. 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, Finance, 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 Legal Aid Board website.