Access Control Policy

Ref: IC014, 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	Access Control Policy
Current Version	v1
Document Reference Number	IC014
Date Effective Until	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	31/05/2024	Full Review	Brian Moss	Gareth Clifford

1. Purpose

This Access Control Policy (or Data Access Control Policy) is the Legal Aid Board's policy governing how staff gain access to and use client and staff personal data and confidential business and commercial data held by the Legal Aid Board, in the course of fulfilling their work tasks.

The data processed by Board employees belong to the Board with the exception of staff members' own personal data. The Board is mindful of its statutory obligations under GDPR and the Data Protection Acts 1988-2018 to ensure that all data it holds are secure and only accessed where needed for a designated business function. The personal data collected concerns individual clients, staff, and contractors. Therefore, the data shall only be used for the purpose stated at the time of collection. The exception is if there are legal requirements for other use and processing of the data.

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 and relevant civil service circulars, including Circular 26/2004 'The Civil Service Code of Standards and Behaviour'. Failure to comply with any part of this policy may result in disciplinary action in accordance with the Civil Service Disciplinary Code (Circular 19/2016).

Access to Board networks, domains, directories, and systems and Board-issued devices their use and management by staff must be in line with GDPR principles and the Board's Acceptable Information Technology Usage Policy and Blended Working Policy. An overview of GDPR principles is provided in the Board's Data Protection Policy. All Board data policies are available at www.legalaidboard.ie. The Board's Blended Working Policy is available to staff on the internal iLAB platform.

3. Definitions

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

Data: The Board possesses two types of data. These carry different obligations and securities and access entitlements and procedures as a result.

Public data includes data that the Board publishes freely, such as contact details, research findings, news, and social media posts. Where the Board publishes caseload data this will remove personally identifiable data and use aggregated information only.

Restricted data covers that information the Board will not generally disclose on its own initiative. These include but are not limited to HR, financial and contractual matters, client details, policy decisions, and procedures.

Data the Board uses are available in hard and soft copy formats. Hard copy formats are those a staff member can see/ hold in their hands and includes print outs and original items in and relating to client, financial, HR, research and other corporate functions of the Board. Soft copy formats are those a staff member can see on the screen of a Board-issued device that has access to the Board's managed ICT services.

Data repositories: the Board stores data in four main ways. These are digital storage locations personal to each staff member and shared drives specific to a business unit/area; business systems for legal aid, mediation and supporting corporate matters; email, voice, and messaging systems; and databases such as those for HR, Facilities, and Finance roles.

4. Roles and Responsiblities

The HR unit: has responsibility for granting and revoking initial access to managed ICT services. Where necessary it will decide all requests for altering access to all Board-provided networks, communications, and ICT systems in conjunction with input from the IT Unit. Otherwise the IT Unit will decide on any alterations to managed ICT service access. Those services to which access will be decided include but are not restricted to:

- login;
- email and messaging systems;
- business systems (e.g. case tracking systems); and
- telephone Directory.

IT Unit: maintains all of the Board technologies, devices and all managed databases / systems. The IT Unit implements any HR decision to grant, maintain, increase or reduce a staff member's access to data / directories held by the Board. It is also responsible for ensuring that all controls remain fit for purpose, offering the protections expected under GDPR, to minimise risk to the Board and to maintain the Board's standing.

Directors: Directors head up Directorates. Every six months they review access lists circulated by HR, ensuring that individual staff access to the systems under their remit is appropriate. The process for this is set out in Appendix 1.

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. The section manages subject

access requests, breaches, and conducts data protection impact assessments where needed. The section also acts as the main contact point for the Data Protection Commission, the Irish supervisory authority on data protection.

The Data Protection section has no access to client or business data, in line with the GDPR principles of protecting data. The section is generally reliant on the other business units of the Board, who act as data owners and administrators, to confirm data and to respond to data subjects' requests. A business Unit looking to involve the Data Protection section in a matter and disclose data to it should notify this in writing at the earliest opportunity via a manager at Assistant Principal Officer / Managing Mediator / Managing Solicitor level or equivalent. The Data Protection section will consider requests on a case-by-case basis.

5. Individual Staff Access

General requirements

- In all cases physical and digital access privileges will be based on the principle of "least privilege", that only the most basic access privileges necessary to carry out a designated role are given to staff.
- Access rights will not be provided to staff by default.
- Any data marked as restricted must not be accessed by a staff member unless given prior approval by their manager for a work purpose.
- Where any public data published by the Board is incorrect or misleading, Board staff must report this to the Data Protection section as soon as possible.
- Usernames and passwords provide a primary means through which networked Board data are accessed and locked. The IT Unit issues staff with usernames and passwords to access these.
- Original usernames and passwords and any changes to these should be kept confidential by staff to themselves at all times.
- Staff should aim to create a strong password for their Board and other accounts related to their employment (e.g. NSSO account) and follow IT Unit guidance in setting any password.
- Individual business units may have access to certain standalone databases / systems. These systems will be managed by the IT Unit. Access to these will be determined by unit managers and access credentials for these should not be passed to others without proper authorisation.
- Each Board database, system, or domain has a designated owner and administrator but in all cases will be maintained by the IT Unit. Access to each database, system, or domain must be managed by an administrator. This administrator must maintain a record of all registrations / de-registrations on the domain / system over time and current users at any point in time. The administrator must also have an administration level account that is separate from their standard user account.
- Any change to access in excess of what is originally provided to a member of staff must be decided by the IT Unit in conjunction with the local data owner at Managing Solicitor/ Managing Mediator/ Assistant Principal or equivalent grade or higher.
- All requests for special accounts/ privilege rights must be formally documented and approved by the IT Unit via the AskIT function.
- Any staff member assigned to a matter in which a person known to them personally plays a central role should ask their manager to re-assign the matter. Where a manager decides not to re-assign the matter, a reason for this should be documented.

Staff Changing Employment

The Board identifies three distinct categories of staff in terms of access. These bring different requirements.

New Staff

Staff joining the Board should be set up with basic access to the Board network in advance of their arrival. This will include:

- Email and messaging;
- Flexi;
- NSSO;
- iLAB; and
- Telephone directory.

New staff will also need access to specific directories within individual business units. The procedure for establishing new staff access to such directories is that:

- HR must contact IT to initiate this process;
- HR must inform the relevant business Unit of the new staff member's expected starting date;
- The receiving business Unit lead at Managing Solicitor / Managing Mediator, Assistant Principal or equivalent grade should contact IT on the new staff member's first day to indicate the specific directories / case management systems to which the staff member should be given access.

Staff transferring business area

Staff transferring from one functional area of the Board to another shall be understood as having two phases:

1. removal of old access to their original business area; and
2. granting of new access to their new business area.

Where a staff member is moving, their manager must arrange for data access in that business area to be removed. This should be done in advance by contacting the IT Helpdesk and should be scheduled for the working hour of the final day that the staff member will leave the business area.

Where a staff member moves to a new area, their new manager must arrange access to specific directories. This should be done once the staff member has started in the business area / unit. This should be done by the new manager or by the staff member (with a record of their manager's approval) contacting the IT Helpdesk. Approval for the access will be sought from the new manager.

Staff leaving Board employment

Staff members leave Board employment for a variety of reasons, whether permanently or for a temporary period, such as secondment. In all cases, the following procedures apply:

- All staff retain access to the system until their last day as an official employee.
- All data access should be removed at close of business (17:00 hours) on that final day.
- The exception is where a staff member has breached the IT Acceptable Computer usage policy, this has been signalled to them by HR and an investigation of that breach is underway. In that event, an employee may cease to have access to Board technologies at a point ahead of their final day, as determined by Board management.
- Where the final day(s) of a staff member's time in the Board occurs during a period of leave, their last day will still be the date of their final day as an employee.
- To achieve that, the HR Unit or staff's manager must inform the IT Helpdesk in advance of that date;

- All Board-issued devices should be retrieved before the staff member leaves. If a staff member's final day falls during a period of leave / during a period of sickness, the staff member must arrange to return any Board-issued devices before the leave commences or later at their own cost.

In the case of a staff member moving to a new business area or leaving Board employment, their name/ and or email address must be removed from address books on networked photocopier-printer-scanner devices in the business unit. This should normally be done as soon as the staff member has ceased employment there.

The IT Unit conducts routine auditing of access to all networked domains, systems and databases. In the event that a query arises over access to client or business data, the IT Unit will raise this with the Director Information & Communications, the staff member's line manager and HR Unit as necessary.

Exceptional Circumstances
Exceptional / occasional circumstances may arise where access above what is normally required. Examples include a staff member moving business area but needing to retain access for a defined period of time to assist a unit or to finish a piece of work they had underway before the move.

In such situations, the manager looking to provide the access to the staff member is responsible for clarifying the exceptional basis of the request with the IT Unit, requesting the access from the IT Unit, and also requesting its removal by the IT Unit when the work is complete.

6. Working away from the office

During their employment Board staff may undertake their duties in one of three different arrangements. These are on-site at a Board office, remote working at the site of another organisation (e.g. court building), and blended working from their home.

To facilitate such work, on occasions staff may have a perceived need to remove a document / file from their local office. To that end, each Directorate needs to develop and document the tasks, roles, and contexts that require the removal of files or documents from a Board office. In all cases, removal of any documents/ files from a Board office must be compliant with GDPR through staff doing the following:

- The default position is that a staff member engaged in blended working should access soft copies of any documents they need.
- A staff member may remove documents / files for working remotely (e.g. at court, agreed mediation place).
- No documents or files containing personal, confidential, or commercially sensitive data should be removed from Board workplaces for the purpose of working on them at home.
- A staff member must ensure that any documents/ files they remove from the office for the purpose of remote working, are returned to the local office that same day.
- Where it is not possible to return the documents/ files that day due to some valid reason (e.g. late finishing at a courthouse), the items must be returned the next working day.
- If it is not possible to return a document/ file the next working day, this should be considered in advance of removing them from the office, and discussed with the local manager.

- All items removed from a Board site for the purpose of remote working must be kept secure at all times by the staff member removing them.
- To achieve this, staff must already possess and must use a locked briefcase at all times for holding any Board documents / files when not in use.
- The briefcase must be kept in a secure location.
- Where it is intended to remove any document/ file from a Board office for the purpose of remote working, a note on each document/ file must be recorded by the staff member in advance. This should be recorded in a centrally held log within the local business unit, and reviewed by the local manager at least once each week. This is in line with the internal Board Administrative Procedures Handbook.

These points are also set down in the Board's Data Classification Policy, available at www.legalaidboard.ie.

7. Staff Downloading Board Data

Beyond movement of staff out of Board employment and to new roles across the Board, in the normal course of work, Board staff are given access to varying degrees of client, staff, and contractor data, depending on their business tasks. These data are stored in different digital storage locations. Content and access to the Board's shared digital location will be kept under review by local managers.

In relation to such data staff:

- must only access Board data using their own username and password;
- should only access Board data in line with an authorised task given to them;
- must not download any data with the intention of using it or sending it outside the Board, unless in line with a task that has already been authorised by their manager and the designated data owner within the Board; and
- must safeguard any data downloaded and moved offsite in line with GDPR obligations; and
- any data that is to be moved off-site must be only be done with prior approval from their manager and having first recorded the data that are to be moved.

8. Other Access

Requests to access data, and the monitoring and adjustment of controls around data access are routine expectations of the Board's business. Scenarios in which this is expected to occur are set out below.

IT Unit Staff

The Board's IT Unit is central to the maintenance of the Board's technologies. To do this effectively IT Unit staff are given access to different databases and directories at different times. Where IT administrator accounts with unrestricted access to personal data are created, the following will apply:

- such accounts will be allocated only where necessary and their use will be monitored;
- IT staff will have separate user and administrator accounts;
- IT staff should view only those data necessary to complete their designated task;
- all IT staff access will be monitored and reviewed on a monthly basis at HEO and/ or Assistant Principal level. The method for doing this should follow the procedure from point 6 of Appendix 1;

- multiple independent levels of authentication are used where administrators have advanced access to personal data or where they have access or control of a staff member's account;
- no unrestricted access to personal data will be given to any staff member outside of the IT Unit.

More generally, the IT Unit staff is entrusted with the upkeep of the Board's technologies. Given this, it:

- can alter individual staff usernames for Board purposes and must notify staff in advance of doing so;
- can ask staff to create a new password to access Board networks and staff must comply;
- will only ask staff to accept a new username or create a new password where necessary;
- will limit data access to a "need to know" basis, understanding different user access entitlements and applying appropriate controls to reflect that.

Internal Audit Access

The Board's Internal Audit Unit functions to evaluate and improve the effectiveness of the organisation's governance, risk management, and internal control items. In the course of its work, Unit staff can request access to client and business files, assurances as to local file management and protection practices, and highlight, and make recommendations on any such issues arising.

Board staff must comply with requests from the Internal Audit Unit to allow it conduct their audit work. Where there is a query about the access that should be given, this will be raised to the Managing Solicitor/ Mediator, Assistant Principal or equivalent at the local level and discussed with the Assistant Director Internal Audit in the first instance. The Data Protection section will be contacted. Where agreement is not secured at that stage, the matter will be raised to CEO and/ or Board as necessary.

Board CCTV equipment

The Board makes use of standalone computers through which to store and access CCTV footage from cameras located on its business sites. In relation to these computers the following should be noted:

- No staff member outside the IT Unit should attempt to access such computers;
- The passwords for such computers will be set by the IT Unit only;
- Where necessary, the IT Unit in conjunction with the Data Protection section will sanction and enable computer access to a Board staff member for a particular CCTV task;
- The IT Unit will ensure to alter the password used to access a computer after completion of any designated CCTV task.

Contractor/ Service Provider Access

The Board may provide a contractor/ service provider with access to its network in order to complete a business purpose. In such scenarios, the IT Unit will determine the business need, access requirements, and liaise with the Data Protection section for consideration. The Data Protection section will engage with the service provider as needed and revert to the IT Unit.

Any change to access in excess of what is originally provided to a contractor must be decided by the IT Unit in conjunction with the relevant data owner at Managing Solicitor/ Mediator/ Assistant Principal or equivalent grade or higher. All such requests should be submitted via the AskIT platform.

External Requests

Personal data collected by the Board is primarily intended for access and use by the Board's staff only. Third parties may access personal data for two purposes:

- where the Board enters a formal agreement to transfer information to them for business purposes. The range of agreements where this is permissible is set out in the Board's *Data Protection Policy* available at www.legalaidboard.ie. All agreements must be completed before giving access to any Board systems, data, or domains.
- law enforcement or bodies carrying out an investigation may also request access to Board data. All such requests will be considered on a case-by-case basis.

External requests to access Board data should be directed to dataprotection@legalaidboard.ie or FOI@legalaidboard.ie, whichever is appropriate. Please see www.legalaidboard.ie for information about both functions.

9. Security

The Board operates its technologies and networks by means of various protections. These include:

- password or designated access to all managed systems, databases and directories;
- automatic access locks on pcs, notebooks, and mobile phones after a defined period of inactivity;
- the IT Unit monitoring access to all databases, directories and systems under its management;
- the IT Unit compiling quarterly reviews of access to all databases, directories and systems under its management;
- the IT suspending inactive accounts after a number of days determined by the IT Unit, following confirmation with user's line manager;
- the IT Unit deleting suspended accounts after a period of days of inactivity determined by the IT Unit, following confirmation with a user's line manager;
- the IT Unit taking prompt action on requests to create or change access privileges, passwords and where a breach is suspected;
- the IT Unit ensuring that all new passwords are conveyed to users in a secure and confidential manner, that all passwords require alteration after a period of days determined by the IT Unit;
- line managers and unit leads making timely requests to the IT Unit to change access privileges and to report where a breach is suspected;
- line managers and unit leads must review team member permissions;
- where temporary access is required and granted, it will be removed immediately after completion of an agreed task; and
- if in doubt, a query should be raised via AskIT or via a Managing Solicitor/ Managing Mediator/ Assistant Principal or equivalent to the Assistant Director IT before seeking to grant any access.

In the event of a query over a staff member's use of an account, database, domain or directory, this will be dealt with in accordance with the Board's Acceptable IT Usage Policy. The policy is available at www.legalaidboard.ie.

10. 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

11. Making a Complaint

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

12. 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

The Process for six-monthly review of access lists by Directors is as follows:

1. The Data Protection Section notifies Directors by email of the need to undertake the six-monthly review.
2. Directors receive lists from HR of all staff listed as having access to a digital storage location.
3. Directors/ their designates determine which staff should continue to have access to a digital storage location within their Directorate's area of work and which staff should not.
4. Each Directorate submits a return via the AskIT platform.
5. The return would note any discrepancies between the HR list and current staff lists.
6. The IT Unit forwards the data to the HR Unit.
7. The HR Unit collates the data and seeks any changes to staff access via the IT Unit.
8. The HR Unit informs the Data Protection section of the number of changes sought and to which Directorate. It also informs the Data Protection section of any Directorate that did not reply.
9. The Data Protection section sends any reminders regarding completion of the review.
10. It then collates a summary report intended for the EMT and Board.