Acceptable IT Usage Policy

Ref: IC007, v5

September 2025

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	Acceptable IT Usage Policy
Current Version	V5
Document Reference Number	IC007
Date Effective From	12 September 2025
Date Effective Until	11 September 2026
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	-	New Policy	Data Protection, HR and IT	Broader Management Team
2	-	-	Data Protection, HR and IT	Broader Management Team
3	16/7/2021	Revision across all aspects of use of the Computer Network, E-Mail, Instant Messaging and Internet	Data Protection, HR and IT	Broader Management Team
4	30/4/2024	Full Review	Brian Moss	Gareth Clifford
5	12/09/2025	Full Review	Dr. Ellen Ganly	Dr. Brian Moss

1. Purpose

This is the Legal Aid Board's policy on acceptable use of technologies that are made available to staff to undertake their work. The Board has a statutory obligation under GDPR and the Data Protection Acts 1988-2018 to ensure that all data stored on its computer systems are secure at all times.

The Legal Aid Board uses a variety of technology formats and devices to undertake its work. It makes available to staff some/ all of these technologies to undertake their work tasks. All technologies enable staff to relay information beyond the organisation, whether through the internet or individual persons. This presents opportunities to disclose data either intentionally or by accident or cause damage to the Board's IT network, harm to clients, staff, or contractors, and to the Board's business and reputation.

2. Scope

This policy applies to all functions of the Board conducted by Board staff, volunteers, Processors, or contractors. Failure to comply with any part of this policy may necessitate disciplinary action in accordance with the Civil Service Disciplinary Code (Circular 19/2016).

The policy should also be read in conjunction with relevant civil service circulars, including Circular 09/2019 'The Policy on the Use of Private Email and Other Private Messaging Services' and 26/2004 'The Civil Service Code of Standards and Behaviour'.

3. 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.
- **Legal Aid 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 technologies to complete agreed tasks**.**

4. Roles and Responsibilities

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 Officer role is located in the section and leads on these matters utilising staff support, assistance, advice, and training to enhance organisation-wide compliance with data protection.

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.

Staff must use any Board-issued technologies in a courteous and respectful manner, respecting clients, colleagues, contractors, and the general public around them when doing so.

Staff must use any Board-issued technologies in a safe manner, limiting risks to their own health (e.g. not using a mobile phone while driving) and the health of others.

Staff must use any Board-issued technologies as economically as possible (e.g. mobile phone use, photocopying), except where unavoidable in the course of completing a designated task.

The Legal Aid Board does not pay for any personal devices or costs associated with that device (e.g. phone bill)

Save in exceptional circumstances, staff must not use a personal device for conducting Board business (see section 5.5). In normal circumstances the Board will not pay the bills for using a personal device to undertake Board-related business tasks.

5. Procedures

5.1 Material Staff Receive

All materials that Board staff receive via technologies (e.g. email, mobile phone, video call platforms) for their attention / as part of their designated work in a Unit must be opened, read, evaluated and responded to in accordance with guidance set out in any Board Customer Service Plan and / or Administrative Procedures Handbook or other adopted local business unit procedures in place at the time.

Potentially dangerous material

a) Staff must not launch, detach or save any executable file (e.g. those ending in ".exe" or ".vbs") under any circumstances. A full list of files types is available for staff on the internal, staff knowledge repository, iLAB. Where one of these file types is launched, a staff member should contact the IT Unit immediately.
b) Staff must not open, detach any unofficial file types, applications, or save any unofficial file attachments to any LAB devices (e.g. pc, laptop or mobile phone).
c) Official attachments should be placed in the relevant document library/directory.

Obscenity, child pornography and incitement to hate

Board staff are subject to all legislation regulating internet use, including the provisions regarding obscenity, child pornography, sedition, and incitement to hatred. The Board has obligations under the Child Trafficking and Pornography Act 1997 not to allow any of its systems (mail, internet, etc.) to be used for downloading, distributing or possessing offensive material.

The Legal Aid Board is also obliged to report any violations to the appropriate authorities.

Other offensive and time-wasting material

Unsolicited material can arrive onto LAB devices from many sources. Should a staff member receive material which they find to be offensive, abusive, or time-wasting, they should complain directly to the sender if known and bring it to the attention of the sender's employing organisation/manager, the LAB IT Unit and LAB HR Section, as appropriate.

5.2 Material Staff Send

Staff should view any communication they might send via Board-issued technologies (e.g. email, mobile phone, video call platforms) as effectively being a communication on Board-headed paper. Communications have identifying marks that can be traced back to the location, date, and time of sending. Therefore, staff must adhere to the points below when sending communications via Board-issued technologies.

a) Use SecureMail where material of a personal, private, sensitive, or confidential nature is being sent by email outside of the Board's IT environment.
b) Do not send or request to receive via a Board-issued mobile phone anything that contains confidential and/or personal information regarding the Legal Aid Board, its employees, clients or contractors.
c) Do not send any material that may be offensive or disruptive to others or which may be construed as harassment. Do not make any derogatory comment regarding gender, marital status, family status, sexual orientation, religion, age, disability, race, socio-economic statues or membership of the Traveller community, any item that contravenes the Board's Equality, Diversity, and Inclusion Policy or any comment that could be seen to undermine the dignity of the recipient.
d) Be satisfied that the content of a communication (e.g. email, text) is appropriate for the purpose and, where necessary, approved by a line-manager.
e) Double-check the address/ number of the intended recipient. Once sent, communications cannot be stopped or retrieved. This can create data protection difficulties.
f) Do not send any unofficial graphics or executable files under any circumstances.
g) Do not instigate or forward "junk" emails to users either inside or outside the Board.
h) Do not include personal contact details (i.e. email/ phone number) in work-related communications.
i) Do not send non-business group communications e.g. those that canvass for elections or political parties, or those seeking to procure or to sell goods. The Social and Advertisements sections of the Discussion Forum on iLAB may be used occasionally to communicate with colleagues generally e.g. advertising an item for sale or organising a social event. No commercial, campaigning, or political material may be posted to the Discussion Forum.
j) Do not send communications that knowingly misrepresent the Board.
k) Do not deliberately misspell words or phrases in order to deceive the Board's monitoring software.
l) Do not use a Board-issued technology for personal matters e.g. booking holidays, purchasing goods and services online, or registering on third-party websites (See also 'Timewasting and Resources' below).
m) Do not use another staff member's email account or device. Where a person has a scheduled absence (e.g. annual leave, study leave), they can delegate access to their email account to a colleague during the relevant period. That way the colleague can respond to or act on any time-sensitive correspondence without being given the absent staff member's password. (The instructions for delegating email are available on the IT tile of iLAB.)

n) If intending to be out of office for a sustained period, a staff member should activate their out of office auto-reply (email) or put in place an appropriate message (phone), directing colleagues and customers to another user / general Board contact method.
o) If a staff member is offsite for official business for longer than two days, they should activate their out of office auto-reply, directing colleagues and customers to another user / general Board email address for urgent matters.
p) Staff must not divert a Board-issued mobile phone to a personal phone number.
q) Staff must not put their SIM card from a Board-issued mobile phone into another phone – personal or Board-issued.
r) The rules concerning the distribution of material via Board-issued technologies also apply to any other platforms used by the Board to distribute electronic data, such as Sharefile.
s) All work emails are automatically backed up and are recoverable. All e-mails leaving the Board will have the following text automatically appended:
    - "The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer. It is the policy of the Legal Aid Board to disallow the sending of offensive material and should you consider that the material contained in this message is offensive you should contact the sender immediately and also postmaster@legalaidboard.ie"

5.3 Screening and accessing emails

The Legal Aid Board utilises specialised software to screen automatically all emails for known viruses, attachments etc. The primary purpose of this screening is to protect the organisation from a cybersecurity event for both the protection of data and the maintenance of the network for the provision of Legal Aid Board services. The settings of the monitoring software are such that incoming and outgoing mail may be blocked. A notification of the blocked email will be sent automatically to the intended recipient who may contact IT for the email to be release. IT will conduct a review of the blocked email and, if non-hazardous to the organisation, will release the email to the intended recipient.

Accessing emails in the event of a potential policy breach

In the course of its work, the IT Unit may identify evidence to suggest that there has been a breach of this Policy; other Board policies, such as the Data Protection Policy; or wider Civil Service policies such as Code of Standards & Behaviour. In this instance, the matter will be escalated to the Director of Information & Communications, who will engage with the Director of HR. The Director of HR will consider and determine whether an investigation is required, and may seek further information from the Director of Information & Communications as part of that consideration

The IT Unit does not read an individual's mail or open mailboxes (or hard disk, network drive, mobile phones and relevant backups). There are exceptions to this:

a) On request by the staff member through AskIT@LegalAidBoard.ie. For example, to put in place an out-of-office message for a staff member who forgot to do so while on leave and where requested by the staff member themselves.
b) a MailMeter request that is submitted in line with this policy (see below);
c) the Board's screening software, or a complaint from an individual, leads the IT Unit to believe that a particular mailbox contains material that is dangerous or offensive, once authorised to do so; or

d) there is evidence to suggest that there has been a clear breach of this Policy or other Board policies, once authorised to do so.

Opening mailboxes for investigation (or hard disk, network drive, mobile phones and relevant backups) requires authorisation in writing by the Director of HR, in consultation with the Director of Information & Communications. This consultation is to ensure compliance with information security, GDPR, Board approved policies, such as the Access Control Policy, and to ensure due process and fair procedures for any potential investigation. These authorisations can be delegated to respective Assistant Directors from the respective Directorates. As well as the individual's mailbox, the hard disk, network drive, mobile phones, laptops and relevant backups may be searched as a routine part of that process. Where investigation finds that a problem exists, it will be reported back to the HR Directorate.

Where the problem concerns material such as a virus or an unauthorised .exe file which can damage the network or cause client data to be compromised, the IT Unit will suspend a staff member's email account and inform HR of same. The IT Unit will conduct an cybersecurity incident investigation with appropriate expert external vendors, where appropriate and generate a report for consideration by the EMT. HR will consider the findings and determine if further investigation or action is required.

Accessing emails for other reasons

All emails held by the Board are Board data, not the personal property of the staff member in whose email account they are stored. Consequently, if a member of staff is absent or has recently left, and the line manager is of the view that the email account contains emails of a critical or urgent nature, a request can be made by the local Managing Mediator/ Solicitor/ Assistant Principal in writing to the Director of HR to grant the manager access to the email account in question. This should be done in consultation with the Director of Information & Communications so as to ensure compliance with information security, GDPR, and other Board approved policies. These authorisations can be delegated to respective Assistant Directors from the respective Directorates. All such requests will require that the following must be considered:

a) **Lawful Basis for Processing**: There must be a lawful basis for processing the personal data contained within the emails, such as the legitimate interests of the organisation (e.g., to continue business operations, fulfil contractual obligations, or secure the organisation's assets).
b) **Purpose Limitation**: Access should be limited to specific, explicit, and legitimate purposes. For example, retrieving documents related to ongoing projects or business transactions that the former employee was handling.
c) **Data Minimisation**: The access should be limited to what is necessary for the purposes. Not all emails may be relevant, so access should be restricted to only those that are necessary for the task at hand.
d) **Confidentiality and Security**: The Legal Aid Board must ensure that the data is handled confidentially and securely, with access granted only to those who genuinely need it to perform their job duties.
e) **Transparency**: The former employee should be informed that their email might be accessed after their departure for specific business reasons, typically through a privacy policy or contract)
f) **Time Limitation**: Access to the former staff member's email account should be for a limited time, necessary to complete the intended purpose.
g) **Documentation**: The organisation should keep records of the decision-making process that led to granting access, what was accessed, by whom, and why, to demonstrate compliance with GDPR if challenged.

5.4 MailMeter

As a Data Controller under Data Protection Acts 1988-2018 and the GDPR, the Board is required to know where and how personal data are stored. To assist in this, the Board has an advanced email search tool called 'MailMeter', which provides capabilities for archiving, compliance auditing and forensic searching of email communicationsIt is a crucial tool for ensuring the integrity and retrieveability of email data in compliance with legal and regulatory requirements. Searching for emails via MailMeter is prohibited except where it is necessary for complying with Data Protection or other obligations or requirements such as an investigation; and only if the following procedures are taken:

a) The MailMeter request form (Appendix 1) has been completed;
b) Managing Solicitor / Managing Mediator/ Assistant Principal grade or equivalent, or higher must the request for the search; and
c) The request form is submitted to the Knowledge & Information Unit (Assistant Director) by the applicant.
d) The Assistant Director will support the applicant in refining the request, and, if satisfied, will forward to Assistant Director of HR for a second approval.

Once the above process is followed, the relevant staff members assigned to the duty will be authorised to carry out a search. The staff member assigned will be entitled to access the data for the purpose of complying with the search request. Additionally, the staff member compiling the request will pass any final material located to the Data Protection / FOI section for review and/or to redact the data. After which, the information will be released, through MailMeter, to the requestor. Mailmeter keeps an audit log of user activity.

5.5 Security

Use of SecureMail

The Board has obligations under the Data Protection Acts to keep personal and sensitive data secure. Staff should ensure that all email containing personal, private, sensitive or confidential data is encrypted when being sent outside the organisation. Sending via secure mail ensures that the email is encrypted.

For more information on Secure Mail and sending an email securely, staff should review the instructions 'How to send a secure email' posted on iLAB.

Usernames and Passwords

Board staff members are responsible for the use of the technologies granted in their name. The main protection for this is via staff having a username and password. In relation to usernames and passwords:

a) Staff should make their password difficult to guess.
b) Passwords should not be shared with anyone or generally visible/ available to others.
c) The IT Unit staff will never ask staff for their password over the phone unless it is necessary as part of resolving an issue that the user has already brought to the attention of IT Unit. However, where a staff member disclosed their password to IT, it should be changed immediately after the IT issue is resolved. IT queries are logged at **AskIT@LegalAidBoard.ie** for transparency.
d) If a staff member believes that someone has become aware of their password, they must change this as soon as possible.

e) Usernames and passwords must not be written down and stored with or near any Board-issued device. They should be destroyed once memorised.

Preventing Disclosure

Disclosure of Board data can create difficulties for clients, staff, contractors and the organisation. To that end, staff:

a) must not leave their Board-issued devices (e.g. pc, laptop, mobile phone) unattended without securing them by password, signing off, etc;
b) should view work communications on Board-issued devices only, not on personal devices;
c) should only use their Board-issued device to send business-related items, not personal devices;
d) should not save private contact details (e.g. email addresses or phone numbers) onto Board-issued devices; and
e) should ensure that their device screen cannot be seen by unauthorised individuals. This applies when working in LAB offices, offsite including on public transport, and at home.

In all scenarios remember, Leaving it? Lock it!

Access

All files and folders on the Board's network contain customised security permissions to ensure they can be protected, backed up on a nightly basis, and restored if necessary. These permissions are not to be changed by any person other than an authorised member of the IT unit.

Where a staff member moves within the Board they should no longer try to access or have access to systems, network drives, or data that are not pertinent to their new role. The exception is where retention of access is required for a legitimate work reason, as noted above.

Firewall

Users accessing the internet through a device attached to the Board's network must do so through an approved internet firewall or other security device. Bypassing the Board's computer network security by accessing the internet directly by modem or other means is strictly prohibited.

Virus protection

Files obtained from sources outside the Board, including files downloaded from the Internet, news groups, bulletin boards, or other online services and files attached to e-mail messages may contain computer viruses that could damage the Board's technologies. While the Board is continually upgrading its virus protection infrastructure, if a staff member **suspects that a virus / ransomware etc. has been introduced into the Board's network, they should notify the IT Helpdesk immediately at AskIT@LegalAidBoard.ie**

Cyber Threat Awareness and Cyber Security Awareness Training

The internet is not a secure environment. To limit the effects of this, the Board will provide all staff with access to cyber security awareness training, such as that provided by OneLearning. Staff must complete any Board-provided refresher training when provided. Additionally, staff should:

a) not give out more information by e-mail or via the internet than is necessary to fulfil their work purpose;
b) be wary of websites / correspondence that request more data than is necessary for accessing the site, making a transaction or which do not state why they require data. The Board is not liable for any loss that may result from staff giving out their personal details and having these abused; and
c) not give out information on IT systems or resources over the Internet or through e-mail without prior authorisation from the IT Unit.

Use of external email accounts, mobile phones and instant messaging accounts

Email accounts, mobile phones and instance messaging accounts are provided to all staff for work purposes only. To avoid any risks to clients or colleagues, the following should be observed:

a) Staff are not permitted to transfer or receive personal data relating to staff, clients, contractors, etc. using their personal email / personal phone (calls/texts) / instant messaging accounts (e.g. Gmail, Hotmail, Yahoo, WhatsApp, Viber etc.).
b) Staff are not permitted to engage with staff, clients, contractors, etc. using their personal email / instant messaging accounts (e.g. Gmail, Hotmail, Yahoo, WhatsApp, Viber etc.).
c) Where it is necessary to communicate with a third party on a matter relating to an applicant or client, information should only be sent using a secure encrypted service, such as SecureMail.
d) Where a member of staff has not been given an LAB-issued mobile device, this may not in itself be used as a justification for using a private email, private phone (calls/texts) or private messaging service.
e) Use of external email should never be used to circumvent the recording of information in the appropriate location within the Board, or to otherwise circumvent the Board's internal controls.
f) The Government has identified exceptional circumstances[1] in which it may be necessary to use a private email account or other private messaging service to conduct official business. In such exceptional circumstances, any resulting correspondence must be forwarded to the staff member's Board-issued email account and be deleted from the private account at the earliest possible opportunity. The Board has adopted the position that this will apply in respect of the use of all mobile devices (e.g. laptops, mobile phones, etc.).

5.6 Timewasting & Resources

Board network resources such as storage space and capacity to carry traffic are not unlimited**.** Consequently, a staff member must not deliberately perform acts that waste their own or a colleague's time or technology resources. These acts include:

a) Playing games.
b) Online chat groups, email chat or social media.
c) Uploading/Downloading large unofficial files.
d) Accessing streaming audio/video files that is not related to the work of the Board, for example listening to music or watching movie clips.
e) Forwarding audio/video files to colleagues.
f) Creating unnecessary non-business-related loads on network traffic.
g) Participating in mass non-business-related mailings such as chain letters.
h) Sending unofficial attachments.
i) Making personal online purchases of goods or services during working hours.
j) Conducting private, commercial/ charitable activity.
k) Using the 'Everyone' email group to circulate personal views on a topic or for non-work related items.

5.7 Financial Implications

Staff must not download any material/software for which a registration fee is charged without first obtaining the express written permission of the Board. Only software installed by the IT Unit and therefore listed on the Board's Assets Register, is deemed to be legally sourced by the Board and covered by the appropriate licence agreement. No other software is approved for use on any of the Board's technologies.

[1] Policy on the Use of Private Email and Other Private Messaging Services, Circular 09/2019

5.8 Internet Browsing

Internet access at work is granted on the basis that it is used solely for the purpose of conducting Legal Aid Board business and that it supports the goals and objectives of the Legal Aid Board. Any form of internet information exchange such as file transfer, download of files or web page publishing is to be used for sanctioned business and communications purposes only.

The IT Unit has deployed software that monitors internet access. This software produces reports that can be requested under the Freedom of Information Acts. The reports are monitored regularly and display the details of the user, where and when the site was visited, and the pages accessed during the visit. The use of Internet browsing will be monitored randomly to ensure the integrity and security of the Board's networks and data and that the business use policy is adhered to. The Legal Aid Board will prohibit Internet access if it deems that security has been compromised, or that this Policy has not been adhered to.

Please note that in relation to accessing the internet from Board-issued devices, staff must not:

a) Visit web sites which contain racist information (unless business related).
b) Visit internet sites that contain obscene, pornographic or other offensive material.
c) Visit sites of social content such as Facebook, Twitter etc. unless your official duties include the maintenance of a Board account on such sites, or where you are carrying out a direction of a Court to communicate with a person through such channels.
d) Upload any data to the internet unless it is business related.
e) Make or post obscene, indecent, racist or offensive remarks or comments on the internet nor should you entice others to do so.
f) Solicit email or other internet-based services which are not directly business related or for personal gain.
g) Transmit any material that is defamatory, or which is intended to offend, annoy, harass or intimidate another person or persons.
h) Express any personal opinions as being representative of the Legal Aid Board, whether in a private email or a public Internet forum.
i) Breach any copyrighted material through its transmission, upload or download.
j) Publish or otherwise reveal any commercially sensitive information relating to the Legal Aid Board or any company with which the Legal Aid Board has or had contractual agreements in the past.
k) Circulate any material that may bring the Board into disrepute.
l) Download any software, electronic images, large files, streaming or audio files, screensavers, games, wallpapers, backgrounds, video files or generally any multimedia files which are non-business related.
m) Access external email accounts (e.g. Gmail, Hotmail, Yahoo etc.).
n) Access anonymous redirector sites.
o) Use another user's ID and password or Board-issued device in order to circumvent Legal Aid Board security policies.
p) Attach any device or phone to their Board-issued pc in order to gain direct and unmonitored Internet access.
q) Attempt to access the dark web.

Failure to follow the above will be reported to the HR Unit. The Legal Aid Board is also obliged to report any illegal or criminal violations to the appropriate authorities.

5.9 Mobile Devices

Board staff have at their disposal several mobile devices, such as laptops and mobile phones. While these provide flexibility for work, they also increase the risk associated with storing data securely. While the Board IT Unit will ensure that the correct configuration is installed on all portable devices, individual users are responsible for ensuring the integrity of the configuration. Staff can ensure this by complying with the following in relation to Board-issued devices:

a) The IT Unit can request the return of mobile devices at any stage for audit/ other reasonable purposes and holders of portable devices must co-operate with any such request;
b) In the event of the loss, theft or damage of a Board-issued device, a staff member should immediately notify their manager, the IT Unit at AskIT@legalaidboard.ie and the Data Protection section at dataprotection@legalaidboard.ie;
c) USB sticks and other comparable memory devices are prohibited for use on the Board's network unless provided by the IT Unit and then only if there is a business need that can't be mitigated by other means e.g. ShareFile. This will be determined on a case-by-case basis with information security, cyber security, and GPDR forming the basis of any decision making These devices will be encrypted. The devices must be returned to the IT Unit once the reason for use has been completed. It is the staff member's responsibility to comply with this.
d) Not load any unauthorised, unlicensed, or unofficial software to any portable device;
e) Not allow unauthorised personnel to use it (e.g. family members);
f) Prevent damage through misuse;
g) Not leave a device unattended in public places;
h) Turn off / lock it when not in use;
i) Must store it securely when travelling or not in use;
j) Must store it out of plain sight if left in a car;
k) Must cover any cost in returning a Board-issued device to the Board where they have not done so before leaving Board employment;
l) Not attempt to remove software or passwords assigned to the portable device;
m) View Board data on it only when out of view of unauthorised personnel (i.e. public transport while travelling for work reasons, or other public places like courts)
n) From time to time, it may be necessary for a member of staff to borrow a portable device from a colleague in the same office or unit. Where this is done, the device should be returned to its original keeper without delay once the task for which it is borrowed has been completed; and
o) A C&AG audit may require the Board to confirm that a member of staff has the equipment assigned to them in the assets register. To assist in this, any long-term re-allocation of a device from one staff member to another should be reported to the IT Unit.
p) Not swap SIM cards, either with colleagues or a Board-issued SIM card for a personal SIM card.
q) Must not provide or agree to take another staff member's phone for more than a once-off exceptional use.
r) Not enter into any contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
s) Not create, download, host or transmit (other than for properly authorised and lawful purposes) pornographic, offensive or obscene material (i.e. information, images, video clips, audio recordings etc), which could cause offence to others.
t) Not retrieve, create, host or transmit any material which is designed to cause annoyance, inconvenience or needless anxiety to others;
u) Not retrieve, create, host or transmit material which is defamatory;

v) A member of staff should only have in their possession as many Board-issued devices, as have been official assigned to them for business purposes.
w) Returning it to the IT Unit before leaving the employment of the Board;
x) For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
y) For any activity that would compromise the privacy of others;
z) For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the Legal Aid Board or others;
aa) For any activity that would intentionally waste the Legal Aid Board 's resources (e.g. employee time and IT resources);
bb) For any activity that would intentionally compromise the security of the Legal Aid Board's IT resources, including the confidentiality and integrity of data and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
cc) For the installation and use of software or hardware tools which could be used to probe, and / or break the Legal Aid Board IT security controls;
dd) For the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within the Legal Aid Board or elsewhere;
ee) For creating or transmitting "junk" or "spam" emails. This includes unsolicited commercial emails, chain-letters or advertisements;
ff) For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.
gg) This should not be seen as an exhaustive list. Other examples of unacceptable use of Legal Aid Board mobile phone devices include any act that would be inconsistent with the duties and responsibilities of the staff member as an employee of the Board.

5.10 Shared portable devices

Where a portable device (e.g. tablet device) is not for the sole use of an individual member of staff but is assigned to a Unit / section, a section owner must be identified. The relevant Director is accountable. Tablet devices are only provided in specific circumstances (e.g. use of a specific software such as a video-conferencing software for work related reasons) and will not contain any ability to record or retain client data. The portable device may or may be required to connect to the LAB Network.

The section owner will be responsible for:

a) Ensuring the portable device(s) are only issued to authorised staff. These devices will be encrypted;
b) Keep a record of who was issued a portable device(s) for use;
c) Inform anyone who uses a portable device(s) of the individual responsibilities; and
d) Return any mobile device(s) to IT if requested.

5.11 Remote access

Remote access is granted primarily on the basis of the Blended Working Policy. Some staff may not wish to utilise the Blended Working Policy so as to work from home but still require remote access to undertake their role; for

example, solicitors undertaking work in the courts. Board staff granted remote access when out of the office / when hybrid working must only use the access for their work tasks and not provide it to unauthorised personnel.

5.12 Staff leaving Board employment

All staff retain access to Board technologies until the end of their last working day as a Board employee. There are two exceptions to this. The first is where a staff has been on prolonged absence from work. Such accounts are suspended unless requested by the staff member's line manager. The second exception is where a staff member has breached this policy prior to their final working day, this breach 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.

5.13 Access to technology and devices

A staff member requesting a new/ replacement device should complete the form at Appendix 2. This should be sent to the IT Unit via **AskIT@LegalAidBoard.ie.**

The Board reserves the right to disable or block features on the Board network, domains, registries, and devices.

5.14 Technology replacement and disposal

The IT Unit will determine the functional / obsolete nature of all Legal Aid Board technologies. The Unit will also determine their removal / replacement. Where a staff member believes that a Board issued technology is not functioning as intended, they may require replacement, this should be reported in the first instance via **AskIT@LegalAidBoard.ie.**

Devices will be recycled in accordance with the requirements of the Waste Electrical and Electronic Equipment (WEEE) directive. Staff members must return their devices to the IT Unit.

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

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

7. Making a Complaint

A person dissatisfied with the Board's response to matters relating to its Acceptable IT Usage 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 EMT 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- Request for MailMeter Search

Request for MailMeter Search	
Requesting Directorate	
Reason for Request (e.g. FOI, Discovery, Investigation)	
Requested by:	
Date of Request:	
Search Criteria – i.e. Specific Search terms in body of email, subject heading, @domain.ie or other email addresses (to or from)	
Date Range:	
Who it should be released to:	
Signature of Knowledge & Information Assistant Principal grade or higher	
Signature of HR; Assistant Principal grade or higher	
Date of signature	
For Completion in IT Unit	
Date Search Conducted:	
Search Conducted by:	
Search Reference No (if applicable)	

Details of Search Return: (resources searched, no of hits, general notes)	
Signature of IT Unit, Assistant Principal grade or higher	
Date of signature	

Appendix 2- Device Request Form

Applicant Full Name	
Law Centre/Mediation Office/ Unit	
Work Address	
Home Address (if not being delivered to the office address)	
Contact Number	
Device Type	Mobile ☐ Laptop ☐ Other ☐ specify below _____
New Connection	Yes ☐ No ☐
Upgrade Request *	Yes ☐ No ☐
Network Username	
Network Password	
Date of Request	
Request approved by: Name of Line Manager	

*Note: To be eligible for a phone upgrade you must have had the same phone form a minimum of 2 years. Completed requests to be emailed to AskIT@legalaidboard.ie email address.