



UNITED REPUBLIC OF TANZANIA
TANZANIA LIBRARY SERVICES BOARD



Integrated National Digital Library System Privacy Policy

Mobile application and web portal

Version 1.0 | Last updated 12 October 2026

Effective date 20th October 2026

Privacy at a glance

The Tanzania Library Services Board (TLSB) processes personal data to provide library services, administer accounts, protect users and comply with applicable laws. TLSB does not sell personal data or use it for third-party targeted advertising.

Subject to applicable law, you may request access to or correction of your personal data, exercise other applicable data protection rights, and request deletion of your iNDLS account and associated personal data through the available application, website or contact channels.

Contents

1. About this Policy
2. Who Is Responsible for Your Data
3. Information We Collect and Its Sources
4. How We Use Information and Protect Reading Confidentiality
5. Legal Bases, Consent and Communication Choices
6. App Permissions, Cookies and Analytics
7. Sharing, Payments and External Services
8. Storage and Transfers Outside Tanzania
9. Retention and Deletion
10. Children and Young Users

11. Security and Personal Data Breaches
12. Your Rights and Account Deletion
13. Automated Functions and Changes to This Policy
14. Contact and Complaints

1. About This Policy

The Tanzania Library Services Board (TLSB) operates the Integrated National Digital Library System (iNDLS). This Privacy Policy explains how TLSB collects, uses, stores, discloses, protects and deletes personal data when you use the iNDLS mobile application (the “App”), the iNDLS web portal or digital library services provided through these platforms.

Personal data means information relating to an identified or identifiable individual. It includes account information, contact details, technical identifiers and library activity that can be linked to an individual.

This Policy applies to registered and prospective members, readers, students, children, researchers, authors, publishers, library professionals and representatives of participating institutions whose personal data is processed through iNDLS.

Some external services accessible through iNDLS may be independently operated and governed by separate privacy notices. Where an external service collects additional information or processes personal data for purposes not adequately explained in this Policy, the relevant notice will be provided where required.

TLSB processes personal data in accordance with applicable Tanzanian data protection legislation, including the Personal Data Protection Act, No. 11 of 2022, Chapter 44; the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023; the Tanzania Library Services Act, Chapter 102, R.E. 2023; and other applicable laws.

Where a mandatory legal requirement differs from this Policy, the applicable law prevails.

2. Who Is Responsible for Your Data

TLSB is the data controller for personal data processing activities for which it determines the purposes and means of processing.

A data controller determines why and how personal data is processed. A data processor processes personal data on behalf of a controller and in accordance with its documented instructions.

TLSB may engage service providers to operate, maintain, secure and support iNDLS. Such providers must be subject to appropriate contractual, confidentiality and security obligations and may process personal data only as authorized and permitted by applicable law.

Where another organization determines its own purposes and means of processing, it may act as an independent data controller and is responsible for meeting its own legal obligations.

The TLSB Data Protection Officer is the designated contact for privacy enquiries, data subject requests and complaints. Contact details are provided in Section 14.

3. Information We Collect and Its Sources

The personal data collected depends on the services you use, your membership category and the features available to you.

Registration and service forms identify the information required to provide a particular service and, where applicable, information that is optional. If you do not provide information necessary to verify eligibility or deliver a requested service, TLSB will explain the resulting limitation. Declining optional information or permissions will not prevent you from using unrelated services where they do not depend on that information or permission.

Information category	Information collected
Identity and membership	Name, gender, nationality, username, membership number, membership category, account status, preferred library, digital membership identifier and QR code. Age or date of birth may be collected where necessary for eligibility, age-appropriate services or child protection.
Contact and profile	Email address, telephone number, postal address, language preferences and notification settings. A profile photograph may be collected if you provide it for a supported feature.
Library activity	Searches, saved items, favorites, reservations, loans, returns, renewals, due dates, fines and access to electronic resources, where such records are generated or retained by the service.
Payments and subscriptions	Service or subscription selected, billing or control number, amount, transaction reference, receipt, payment date and payment status.
Communications and support	Enquiries, messages, requests, feedback, complaints, attachments and records of assistance provided.
Technical and security data	IP address, device type, operating system, App version, language settings, access times, session and authentication records, login attempts, feature usage, diagnostic and crash records, and notification tokens where notifications are enabled.

Identity documents and sensitive personal data

An identity document or other official identifier will be collected only where necessary for a specified and lawful purpose. The applicable requirement will be explained at the point of collection.

Where information constitutes sensitive personal data under applicable law, TLSB will apply the additional legal conditions and safeguards required for its collection, use, storage and disclosure.

Sources of personal data

TLSB obtains personal data:

- Directly from you when you register, complete forms, use services or contact TLSB.
- Through technical records generated when you use iNDLS.
- From participating libraries, schools or other institutions where necessary for membership administration or service delivery.
- From a parent, guardian or authorized representative where appropriate.
- From payment providers and other integrated service providers where necessary to provide a service you request.

Where personal data is obtained from another source, TLSB will provide the notice required by applicable law and take appropriate steps to ensure that the collection and subsequent processing are lawful.

Payment information

Payment credentials entered directly into a payment provider's service are handled by that provider in accordance with its applicable privacy and security arrangements. TLSB receives the transaction information necessary to confirm payments and administer the relevant service.

Never send your password, mobile-money PIN, one-time verification code or complete payment-card credentials to TLSB through email, telephone, messaging or other support channels.

4. How We Use Information and Protect Reading Confidentiality

TLSB processes personal data for specified and lawful purposes, including:

- Registering and authenticating users.
- Administering membership and digital identification.
- Managing borrowing, returns, renewals, reservations, due dates and fines.
- Providing access to electronic resources and digital library services.

- Confirming payments and administering subscriptions.
- Responding to enquiries, complaints and support requests.
- Sending essential service notices, reminders and security alerts.
- Maintaining system functionality, troubleshooting faults and improving service reliability.
- Preventing unauthorized access, investigating suspected misuse and protecting users and systems.
- Meeting applicable legal, financial, audit and records-management obligations.
- Producing statistical reports and planning inclusive library services.

Gender and nationality information

TLSB may use gender and nationality information for lawful statistical reporting, service planning and evaluation of access to library services. This can help identify participation gaps and inform inclusive service delivery.

Where individual identification is unnecessary, TLSB will use aggregated or anonymized information for reporting and analysis. Personal data will not be used for an incompatible purpose merely because it is available in the system.

Reading confidentiality

Searches, reading interests, borrowing histories and access to particular resources may reveal private or sensitive information about an individual.

TLSB therefore restricts access to identifiable library activity records to authorized personnel who need the information for a legitimate service purpose, security function or lawful obligation. Such records will not be publicly disclosed or used for unrelated purposes without an appropriate legal basis.

Where information is needed for service monitoring, research, reporting or planning, TLSB will use aggregated or anonymized information whenever individual identification is unnecessary.

Bibliographic and publication information

Where iNDLS supports ISBN, ISSN, ISMN, legal deposit or national bibliography services, TLSB distinguishes publication metadata intended for public discovery from private account, contact and payment information.

Information submitted for cataloguing or bibliographic purposes may be publicly accessible where that is part of the relevant service. TLSB will explain which submitted information is intended for publication or public discovery.

TLSB does not sell or rent personal data and does not use personal data for third-party targeted advertising.

5. Legal Bases, Consent and Communication Choices

TLSB identifies an applicable lawful basis for each personal data processing activity. The appropriate basis depends on the purpose, the service involved and the requirements of applicable law.

Processing activity	Applicable legal basis
Public library and statutory services	Performance of a function authorized by law, including the Tanzania Library Services Act, where the processing is necessary and legally permitted.
Paid services and subscriptions	Performance of a requested service agreement, where applicable, together with relevant statutory duties.
Accounting, audits and legally required disclosures	Compliance with applicable legal obligations.
Optional features and additional uses	Consent where required by law, or another applicable lawful basis that is explained before processing begins.
Account security and service administration	The lawful basis applicable to the underlying service, security activity or legal duty, limited to what is necessary for the relevant purpose.

Reading this Policy, using iNDLS or acknowledging that the Policy is available does not constitute consent to every form of personal data processing.

Where consent is required, TLSB will request it separately, explain the information involved and the purpose of processing, and provide an appropriate means of withdrawing consent. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

Where processing is based on consent, TLSB will not continue relying on that consent after a valid withdrawal unless another lawful basis independently permits the relevant processing.

Communications

Essential service communications may include:

- Account registration and verification messages.
- Loan, return and renewal reminders.
- Payment confirmations and subscription notices.
- Service interruption and maintenance notices.
- Security alerts and important account notifications.

Optional promotional, awareness or similar communications will be distinguished from essential service messages and will include an appropriate means of opting out where required.

Opting out of optional communications will not prevent TLSB from sending essential service, security or legally required notices.

6. App Permissions, Cookies and Analytics

The App may request device permissions necessary for supported features. Permission requests will be made when the relevant feature requires access to protected device functionality.

Device permissions in the released App

TLSB confirms the released version of the iNDLS App requests the following permissions only, together with the purpose of each permission:

Permission	Type	Required / Optional	Purpose / Feature Requiring Permission
Camera	Android CAMERA / Ios Camera	Optional	To scan QR code membership card for quick authentication and login at library kiosks, and to capture profile photo if you choose to add or update your profile picture
Photos / Media / Files	READ_MEDIA_IMAGES (Android 13+) / READ_EXTERNAL_STORAGE (Android 12 and below) / iOS NS Photo Library Usage Description	Optional	To upload a profile photo from your gallery when you choose to personalize your account. The App accesses only the specific image you select, not your entire library.
Notifications	POST_NOTIFICATIONS (Android 13+) / iOS Notifications	Optional	To display loan due-date reminders, reservation availability alerts, payment confirmations via GePG, and essential security alerts.
Internet Access	android.permission.INTERNET / ACCESS_NETWORK_STATE	Required	Core functionality - Required to communicate with iNDLS servers hosted at NIDC Dar es Salaam, authenticate users, manage borrowing, access e-resources and confirm payments. This is not an optional device permission but a basic connectivity requirement.

Depending on the features actually implemented, permissions may include:

- Camera access to scan a code or capture an image.
- Access to selected photographs or files when you choose to upload them.
- Permission to display notifications.

You can manage optional permissions through your device settings. Denying an optional permission may prevent the related feature from working but should not prevent unrelated services from functioning where they do not require that permission.

The App requires an internet connection to communicate with iNDLS. Network connectivity is distinct from optional device permissions.

The App will not access contacts, microphone recordings or precise location unless a supported feature requires that access and the collection, purpose and applicable consent or permission requirements have been explained.

Where a feature collects personal or device information beyond what a reasonable user would expect, TLSB will provide a clear explanation within the App before the relevant collection begins and obtain consent where required.

Cookies and web technologies

The web portal may use essential cookies or similar technologies to support authentication, session management, necessary preferences and account security.

Any non-essential cookies, analytics tools or tracking technologies must be disclosed, together with their purposes and relevant providers. Where consent is required, it will be obtained before the relevant technology is activated.

TLSB will provide appropriate controls for managing applicable cookie or tracking preferences. Available browser settings may also help users manage cookies, although disabling essential cookies may prevent some portal functions from working.

Analytics and diagnostics

Third-party analytics SDKs (e.g., Google Analytics for Firebase, Facebook SDK, Mixpanel, Appsflyer): NOT USED in the App. No personal data is shared with third-party analytics providers.

Technical diagnostics and usage analytics:

Technical diagnostics may be used to identify errors, assess performance and improve reliability. Diagnostics are limited to:

Internal TLSB crash logs (App version, OS version, device model, error code, timestamp) - without personal identifiers where possible
Server performance logs at National Internet Data Center (NIDC) ((response times, error rates) – aggregated Security logs for failed login attempts and misuse detection.

These internal diagnostics are hosted within Tanzania at NIDC and Dodoma DR site, are not used for profiling or third-party advertising, and are retained for 12 months then securely deleted or anonymized.

The web portal uses internal server logs for performance monitoring, retained and managed under the same retention schedule. If any analytics tool is introduced in future, its provider, purpose, data collected and legal basis will be disclosed here before activation, with opt-out controls where applicable.

7. Sharing, Payments and External Services

TLSB discloses personal data only where the disclosure is lawful, necessary for a specified purpose and proportionate to that purpose.

Recipients may include:

- Authorized TLSB personnel who require access to perform their duties.
- Participating libraries and institutions administering membership or providing requested services.
- Technology providers operating, hosting, maintaining or securing INDLS on TLSB's instructions.
- Payment providers confirming transactions and processing payments.
- Content providers verifying eligibility or access to requested electronic materials.
- Competent public authorities where disclosure is legally required or otherwise lawfully authorized.

Third-party providers used by INDLS

Before publication, TLSB must complete the following register using verified information about the live App and portal. Include every provider that receives personal data, including subcontractors where relevant.

Provider or service	Role and data received	Purpose
Hosting and infrastructure	Provider: Government Data Centre (GDC) / National Internet Data Center (NIDC) managed by e-Government Authority (eGA) Data categories: Full iNDLS database (identity, contact, library activity, technical logs), encrypted backups, session data, authentication tokens. Location: Primary - Kijitonyama, Dar es Salaam, Tanzania. Backup - Disaster Recovery Site, Dodoma, Tanzania. Subcontractor: TTCL provides fiber connectivity only, no direct access to personal data.	Infrastructure hosting, cloud computing, web hosting, server colocation, disaster recovery, physical security, network availability. Ensures data residency within Tanzania per PDPA and e-Government Act 2019.
Payment services	Provider: Government Electronic Payment Gateway (GePG) & Hazina Portal, operated by Ministry of Finance, Tanzania Data: Service selected (membership/fine), control number, amount, transaction reference, payer name as per	Transaction verification, payment processing, reconciliation, issuance of Government receipts, audit compliance per Public Finance Act. TLSB does not store full card/mobile money PINs.

	GePG, receipt number, date, payment status. Bank/Mobile Money: Processors via GePG (NMB, CRDB, T-Pesa, M-Pesa etc.) receive only amount and control number, not library activity.	
Email, SMS or push notifications	Provider: Government Mobile Platform (GMP) managed by eGA & SMTP via GDC Data: Phone number, email address, notification token (FCM/APNS token), message content (loan reminder text, reservation alert, payment confirmation), delivery status, language preference.	Delivery of essential service notices: loan due-date reminders, reservation availability, payment confirmations, security alerts, password reset codes. No marketing via third-party platforms.
Analytics and diagnostics	Provider: NOT USED Data categories: NONE shared with third-party analytics providers. Internal: TLSB internal crash logs (App version, OS version, device model, error code, timestamp) without personal identifiers where possible, server performance logs at GDC aggregated.	Purpose for NOT USED: TLSB has verified that the released App v1.0 does NOT include any third-party analytics SDK (e.g., Google Analytics for Firebase, Facebook Analytics, Mixpanel, Appsflyer). Internal diagnostics used solely to identify errors, assess performance and improve reliability, hosted

		within Tanzania at GDC, retained 12 months then deleted/anonymized. Not used for profiling or targeted advertising.
Digital content and authentication integrations	Provider: TLSB (all managed within Tanzania) Data: Membership number, membership status (active/expired), user category (student/researcher/public), requested e-resource ID/metadata only. No payment details or reading history shared with content providers beyond necessity to verify eligibility.	Verification of membership eligibility and access rights to requested electronic materials, journals, e-books, and national bibliographic resources. Ensures only authorized members access licensed content.
Other integrated services	Provider: NONE Data: NONE	Verified: No other integrated services receiving personal data in released version v1.0. No social media logins (Google/Facebook login NOT used), no third-party maps, no advertising networks.

Service providers acting as data processors may receive only the personal data necessary to perform their authorized tasks. TLSB will put appropriate contractual, confidentiality and security safeguards in place.

An external provider acting as an independent data controller is responsible for its own processing activities and legal obligations. Where users are directed to such a provider, TLSB will identify the provider and make relevant privacy information available where appropriate.

Links to independently operated websites do not place those websites under TLSB's control. However, TLSB remains responsible for the lawfulness of disclosures it makes and for appropriate safeguards when engaging processors.

TLSB does not sell personal data to third parties.

8. Storage and Transfers Outside Tanzania

The Tanzania Library Services Board (TLSB) ensures that personal data processed through the Integrated National Digital Library System (INDLS) is stored and processed within the United Republic of Tanzania. Personal data is not transferred outside Tanzania.

TLSB will ensure that the hosting infrastructure, backup systems, disaster-recovery facilities, technical support arrangements and third-party services used by INDLS comply with this requirement. Appropriate measures will be taken to ensure that personal data is not transferred to, stored in, or accessed from outside Tanzania through any system or service connected to INDLS.

TLSB will periodically review its data storage arrangements, service providers and technical infrastructure to verify compliance with this requirement.

If a proposed change to the INDLS infrastructure or service arrangements would involve transferring personal data outside Tanzania, TLSB will ensure that all applicable requirements under the Personal Data Protection Act, 2022, and the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023, are fulfilled before the transfer takes place. This includes obtaining any authorization or permit required from the Personal Data Protection Commission (PDPC) and implementing the safeguards required by law.

The use of iNDLS does not constitute blanket consent to international data transfers. Where a transfer is legally permissible and additional notice or consent is required, TLSB will provide the necessary information and obtain the required consent before the transfer occurs.

9. Retention and Deletion

TLSB retains personal data only for as long as necessary for the purpose for which it was collected, an applicable legal requirement or another specifically justified lawful purpose.

Retention periods depend on the type of information, the relevant service, applicable records-management requirements and whether a dispute, investigation or legal proceeding requires particular records to be preserved.

The following schedule is completed, approved and verified for live App and portal v1.0 - 20 October 2026.

Record category	Retention period or criterion
Account and profile records	While the account is active and as otherwise lawfully required. On account deletion, associated personal data will be deleted unless a specific lawful retention ground applies. Inactive account period and action: VERIFIED - 60 months (5 years) of no login and no active loan/reservation. Action: (1) Email/SMS notice at 60 months warning of pending deactivation, (2) 90 days grace period to reactivate by logging in, (3) If no response, account deactivated and scheduled for secure deletion within 30 days. After deletion, anonymized statistical record retained (membership number hashed, no name/email/phone). Legal basis: Records Management Policy and limitation period. Notification via GMP and email via GDC SMTP.
Borrowing and reading activity	Identifiable records needed to administer an active loan, return, fine or dispute will be retained until the relevant matter is resolved and any further lawful retention requirement is met. Additional borrowing-history and search-log retention: VERIFIED - Active loan/reservation: retained until return + 14 days for dispute resolution. Borrowing history beyond active transaction: NOT RETAINED as identifiable reading history unless you opt-in to personal reading list feature. If you opt-in, retained while account

	active and you can delete anytime via App > My Reading List > Clear. If you do NOT opt-in, borrowing record anonymized after 12 months from return date (membership number replaced with anonymous ID, no link to name). Search logs: anonymized after 6 months. Purpose: to avoid revealing sensitive reading interests per Library Code of Ethics, while allowing optional personal history if you choose. Active fines/disputes: retained until fine paid and dispute closed + 12 months for audit. Legal basis: Library Services Act and PDPA data minimization.
Payment and financial records	VERIFIED - 7 years from the end of the financial year in which the transaction occurred. Example: Payment on 15 June 2026 → financial year ends 30 June 2026 → retain until 30 June 2033. Data retained: control number, amount, transaction reference, receipt number, date, status, payer name per GePG, service type. NOT retained: full card number, mobile money PIN, CVV. Purpose: accounting, audit, compliance with Public Finance Act Cap. 348, Government Finance Regulations, and BOT requirements. Storage: GePG/Hazina Portal and GDC hosting at eGA GDC Dar primary, Dodoma DR backup, both within Tanzania. After 7 years, securely deleted or anonymized except anonymized statistical totals required for historical reporting.
Support and complaint records	VERIFIED - 3 years after closure of enquiry, feedback or complaint. Basis: Limitation period for civil claims, consumer protection, and administrative review under e-Government standards. Extension: If complaint escalates to legal proceeding, investigation by PDPC, or disciplinary matter, retained until proceeding concluded + 3 years. Data: enquiry content, correspondence, resolution, attachment. Stored at GDC Dar, Tanzania. After period, securely deleted. If anonymized for service improvement, no personal identifiers retained.
Technical security logs	VERIFIED - 12 months from log creation date. Purpose: security incident detection, unauthorized access investigation, breach analysis, system performance monitoring per PDPA Section 29 security obligations and e-

	Gov Act security standards. Data: login attempts (successful/failed), IP address, device type, OS, App version, timestamp, access to sensitive functions, error codes. No reading content in logs. Storage: eGA GDC Dar primary, Dodoma DR, within Tanzania, access restricted to authorized security personnel only. After 12 months, logs overwritten or securely deleted. Aggregated statistics (e.g., total failed logins per month) may be retained in anonymized form beyond 12 months.
Backups and disaster-recovery copies	VERIFIED - Backup expiry, overwrite cycle and deletion procedure: Full backup daily incremental, weekly full backup. Retention: 90-day overwrite cycle. Procedure: (1) Daily backups retained 7 days, (2) Weekly full backups retained 4 weeks, (3) Monthly backups retained 3 months (90 days), then overwritten. Deletion procedure: When account deleted or retention expires, primary record deleted within 30 days, backup copies overwritten within next 90-day cycle. Appropriate controls prevent deleted accounts from being improperly restored: TLSB maintains deletion log (membership number hashed, deletion date, method) at GDC Dar, excluded from restore process. Restoration testing ensures deleted records not reintroduced. Encryption: backups encrypted at rest at GDC with AES-256. Location: GDC Dar primary Kijitonyama and Dodoma DR site, both Tanzania, owned/managed by eGA.

When the applicable retention period expires and no lawful reason for further retention exists, TLSB will securely delete the personal data or irreversibly anonymize it so that it can no longer reasonably be linked to an individual.

Where personal data must be retained for a legal obligation, investigation, dispute or other permitted purpose, TLSB will restrict access and use it only for the purpose justifying retention.

Archived personal data remains subject to applicable legal requirements and appropriate safeguards.

10. Children and Young Users

For this Policy, a child is a person under 18 years of age.

TLSB will apply age-appropriate privacy safeguards to library services provided to children and young users. Information about collection and use of personal data will be explained in language suitable for the child and, where appropriate, the responsible adult.

Where parental, guardian or other legally authorized consent is required, TLSB will obtain and record the appropriate consent before the relevant processing begins. The identity and authority of a person acting for a child will be verified using reasonable and proportionate measures.

A school's involvement does not automatically replace parental or guardian authorization. The legal authority for any consent or other authorization must be established in accordance with applicable law.

TLSB will collect only the information necessary to provide the relevant service and meet applicable legal obligations.

Children's personal data will not be used for third-party targeted advertising or inappropriate profiling.

A parent, guardian or other authorized representative may contact TLSB through the channels in Section 14 to raise a privacy concern or exercise a child's rights, subject to the child's best interests and applicable law.

11. Security and Personal Data Breaches

TLSB implements technical and organizational security measures appropriate to the nature of the personal data processed and the risks associated with its use.

Measures may include:

- Secure transmission using HTTPS or equivalent protected communication protocols.
- Access controls and appropriate authentication measures.

- Protection of stored personal data and authentication credentials.
- Security monitoring and investigation of suspicious activity.
- Backups and disaster-recovery arrangements.
- Vulnerability management, updates and maintenance.
- Confidentiality obligations and appropriate staff training.
- Security requirements for authorized service providers.

Authentication credentials must be protected against unauthorized access and must not be stored in readable form where secure credential storage is required. Access to personal data will be limited to authorized personnel and providers who need it for legitimate purposes.

TLSB will review relevant security arrangements and take reasonable steps to maintain their effectiveness. No electronic system can be guaranteed completely secure.

Users should protect their login credentials, sign out when using shared devices and report suspected unauthorized access promptly.

Personal data breaches

Where TLSB identifies a suspected or confirmed personal data breach, it will assess the incident, take steps to contain and investigate it, document the response and implement appropriate corrective measures.

TLSB will notify the PDPC and affected individuals where required by applicable law and within the applicable time limits. Notifications will contain the information required by law and appropriate guidance on measures affected individuals can take.

Suspected unauthorized access, disclosure, alteration or loss of personal data should be reported using the contact details in Section 14.

12. Your Rights and Account Deletion

Subject to applicable law and the conditions governing each right, you may request to:

- Know whether TLSB processes your personal data.
- Access personal data held about you.
- Correct inaccurate or incomplete personal data.
- Request erasure of personal data where the legal conditions are satisfied.
- Object to or request restriction of processing where applicable.
- Withdraw consent where processing is based on consent.
- Raise concerns about decisions based solely on automated processing where such decisions have legal or similarly significant effects.
- Lodge a complaint with TLSB or the PDPC.

Other rights may apply under applicable law.

How to submit a privacy request

Submit your request through the contact channels in Section 14. TLSB may ask for information reasonably necessary to verify your identity and, where applicable, your authority to act for another person.

TLSB will explain any prescribed form or supporting documentation required by law and, where possible, assist you in accessing the relevant procedure.

TLSB will handle requests within the time limits prescribed by applicable law. Where the applicable regulations prescribe a 14-day period for a particular rectification or erasure application, TLSB will observe that period. Other requests will be handled according to the procedures and deadlines applicable to them.

Where a request cannot be fulfilled, TLSB will explain the lawful reason and any available review or complaint procedure.

Requesting iNDLS account deletion

You may request deletion of your iNDLS account and associated personal data through any of the following routes:

1. The account-deletion feature in the App, where available.
2. The account-deletion page on the TLSB website, where available.
3. Email to **info@tlsb.go.tz** with the subject line **“iNDLS Account Deletion Request.”**

The website and email routes are intended to remain available even if you have uninstalled the App.

Provide your registered email address or telephone number and, if available, your membership number to help TLSB locate and verify your account. Do not include your password, PIN or one-time verification code.

TLSB will verify the request, assess any applicable legal retention requirements and communicate its decision within the applicable period. Where deletion is approved, TLSB will explain the expected completion arrangements and confirm completion when the deletion has been carried out.

Account deactivation alone does not constitute account deletion.

TLSB will also instruct processors acting on its behalf to delete associated personal data where required, subject to applicable legal retention obligations.

What happens after deletion?

Deleting your account ends access to services that require that account. Outstanding loans, fines, disputes or subscriptions may need to be resolved through the relevant service arrangements. TLSB will explain the applicable steps and provide assistance where necessary.

Outstanding matters do not justify retaining unrelated personal data indefinitely.

Deletion of an iNDLS account does not automatically cancel a separately administered subscription or service. Where a separate cancellation process is necessary, TLSB will explain the applicable steps and how to obtain assistance.

Where particular information must be retained for a legal obligation, security, fraud prevention, an investigation or another legally permitted purpose, TLSB will explain the category of information, the reason for retention and the applicable period or criterion, subject to any legal restriction on disclosure.

Retained information will be restricted to the lawful purpose justifying its retention and will not be used for unrelated purposes.

13. Automated Functions and Changes to This Policy

iNDLS may use automated functions to search, sort, match, classify or retrieve library materials and to support routine administration.

Where a feature uses personal activity to generate personalized recommendations or profiles, TLSB will explain the relevant processing, identify the applicable lawful basis and provide choices or safeguards where required.

TLSB will not introduce solely automated decisions that produce legal or similarly significant effects without providing the information, rights and safeguards required by applicable law.

Changes to this Policy

TLSB may update this Policy when services, data processing practices, technology or legal requirements change.

The published version will identify its version number, last-updated date and effective date. TLSB will provide appropriate notice of material changes affecting users' personal data or rights.

Where a change requires new consent under applicable law, TLSB will obtain that consent before commencing the affected processing.

Continued availability of the App or portal does not, by itself, constitute consent to processing for which consent is legally required.

14. Contact and Complaints

For privacy enquiries, requests to exercise data protection rights, account deletion or reports of suspected privacy or security incidents, contact:

Data Protection Officer

Tanzania Library Services Board (TLSB)

Bibi Titi Mohamed Road

P.O. Box 9283

Dar es Salaam, Tanzania

Email: info@tlsb.go.tz

Telephone: +255 22 2150048/9 or +255 22 2151100

Website: www.tlsb.go.tz

INDLS portal: <https://idlibtaifa.tlsb.go.tz>

Please mark privacy correspondence for the attention of the Data Protection Officer.

You may also lodge a complaint directly with the Personal Data Protection Commission (PDPC) through its official website:

<https://www.pdpc.go.tz/>

Contacting TLSB first may help resolve your concern, but it does not prevent you from approaching the PDPC through the procedures available under applicable law.

Document control

- Document owner: Tanzania Library Services Board.
- Responsible office: Data Protection Officer.
- Version: 1.0.
- Effective date: 20 October 2026.
- Review: Periodically and whenever material changes in law, technology or processing practices make a review necessary.