Library of Code, Inc — Platform

Privacy Policy

Version 1.0 · Effective: November 2, 2026

This policy covers the **Library of Code Platform** — your LOCID account, Cloud Services (CSG2), Library of Code Google Workspace accounts, and any other service we offer through your LOCID. We collect data to verify the authenticity of accounts, perform authentication, operate the Platform, and keep it secure. This policy explains what we collect, why, and what your rights are. It should be read together with the Terms of Service.

At a glance

DATA UTILIZATION	YES	NO
Do we sell your data		**X**
Do we share your data with third parties for their marketing		**X**
Do we use service providers to operate the Platform (hosting, storage, email, help desk, AI assistance for staff, Google Workspace — see Sub-processor List)	**X**	
Is the Platform accessed and administered through a third-party chat platform (Discord) that sees your chat identity and messages	**X**	
Is routine internal access limited to staff in the functions that operate and secure the Platform	**X**	
Do we require identity verification (ID document + selfie) for most members		**X** (only for higher-risk capabilities or flagged accounts; see Section 2)
Do we log and monitor activity on the Platform, including recording remote sessions on Cloud Services	**X**	
Do we use your data to build a personalized or advertising profile		**X**
Do we give other members access to your hosted environment or accounts (content you publish is public)		**X**
Do we store data outside the United States (Helsinki, Finland)	**X**	
Do we delete your hosted content and issued accounts when your LOCID is deleted	**X**	

Do we keep account records, logs, and correspondence after your account is deleted (indefinitely, as records — Section 8)	**X**
Can you request a copy, correction, or deletion of your personal data (deletion subject to the exceptions in Section 8)	**X**
Do we disclose data to authorities — only when required by law or legal process, to report child-exploitation material as the law requires, or in an emergency involving risk of serious harm (Section 6)	**X**

This summary is provided for convenience; the full policy below governs and controls in the event of any discrepancy.

1. Who we are

Controller: Library of Code, Inc., a Wyoming (USA) nonprofit corporation recognized as tax-exempt under Section 501(c)(3) of the Internal Revenue Code, governed by a Board of Governors. 30 N Gould St, Ste 21543, Sheridan, WY 82801, USA.

Privacy and data requests: **it@libraryofcode.org** · Legal notices: executive@libraryofcode.org · Support: https://loc.sh/cs-help

2. What we collect

LOCID — identity and account data (all members). Your full name (given and family name, as provided at sign-up), primary and secondary email addresses, identifiers for the accounts you use to access the Platform (including your Library of Code identity and linked chat-platform identity), account metadata such as status, roles, and which Services you have, and authentication events. Providing identity data is required to create an account; without it we cannot provide the Platform.

Technical data (all members). IP addresses, device and browser information, and strictly necessary cookies used for sign-in.

Cloud Services (CSG2) — hosting data (members with hosting). Account metadata such as tier; records of the resources provisioned to you; records of remote-access sessions; activity within your hosted environment (processes run, network connections made); and network and firewall logs. **Remote-access sessions may be recorded, including the commands you enter and the output displayed.** Recordings can capture anything shown or typed in a session, including file contents and secrets. We attempt to filter secrets from recordings but cannot guarantee it — avoid typing secrets on the command line. Also: the files, code, and data you host with us.

Google Workspace accounts (members issued one). The account details of your Library of Code Workspace account and its contents (mail, files, calendar, and other Workspace data), which are processed by Google and administered by Library of Code. Administrators can access, search, export, reset, or delete the account and its contents.

Identity verification data (only when required). Most members never go through identity verification. We may require it before granting higher-risk capabilities (for example, VPN tunnel access), if your account is flagged, or otherwise case by case. Verification is performed by our identity-verification provider, Didit, which collects an image of your government-issued ID, a selfie or short liveness video, and the details it reads from your ID (such as name, date of birth, document number, and expiry). **The selfie/liveness check is biometric**

data, and it is collected only with your explicit consent at the time of verification; if you decline, you simply won't be granted the capability that requires it. Library of Code receives and keeps only the result (pass/fail), your verified name and date of birth, and a verification reference number — we do not receive or store copies of your ID images or selfie. Didit processes the images and biometric data on our behalf under its own verification privacy notice and biometric data policy.

Communications. Your communications with our staff, including support tickets, support requests, and other operational messages.

Data about other people. If you store or host personal data about others (for example, users of an application you run, or people you correspond with from a Workspace account), you are responsible for it as its controller and for having a lawful basis and any required notices; we process it only to provide the Platform. Our network logs may also include IP addresses of people who connect to services hosted on Cloud Services; we handle that data under this policy.

Apart from the biometric check described above (which happens only with your explicit consent), we do not intentionally collect special-category data; do not store or host it unless you have a lawful basis to.

3. Why we use it (and our legal basis)

Purpose	Legal basis
Provide and operate the Platform and its Services (accounts, resources, access)	Performance of a contract
Verify identity and authenticate access	Performance of a contract; legitimate interests (security)
Identity verification for higher-risk capabilities or flagged accounts (ID document)	Legitimate interests (fraud and abuse prevention, protecting members and infrastructure)
Biometric check (selfie/liveness) during identity verification	**Your explicit consent**, which you may decline or withdraw (we then cannot grant the capability that requires verification)
Security, abuse prevention, ToS enforcement, protecting members and infrastructure	Legitimate interests
Operations, reliability, troubleshooting, backups of our own platform records	Legitimate interests
Support	Contract; legitimate interests
Compliance with law and lawful legal process	Legal obligation (where EU/UK law applies); otherwise our legitimate interest in complying with laws that apply to us, including U.S. law

Our legitimate interests are keeping the Platform secure, preventing abuse, enforcing our Terms, complying with the laws that apply to us, and running a reliable free service. We rely on them only where they are not overridden by your rights.

We do not make decisions based solely on automated processing that produce legal or similarly significant effects for you. Automated resource limits may apply to your hosted environment; decisions to suspend or remove an account are made by people. Our staff may use AI tools to help summarize alerts or draft responses, but a person reviews and decides.

4. Monitoring and logging

Because we operate the infrastructure, **activity on the Platform is logged and monitored.** For every member this includes authentication and sign-in events and network logs. For Cloud Services it also includes remote-access sessions (which may be recorded, including commands and output), activity within your hosted environment, and firewall logs. Workspace account activity is logged by Google and visible to our administrators. Some of these monitoring capabilities may not be active for all members at all times.

What this means: activity on the Platform is logged and visible to Library of Code. Do not use the Platform for anything you need to keep private from us. We access logs and content only for the purposes described in Section 3.

5. Staff access

Because we operate the underlying infrastructure, our staff have the technical ability to access, inspect, copy, modify, or delete data and to observe activity. Routine access to member data and logs is limited to staff in the functions responsible for operating and securing the Platform, and only to the extent their role and responsibilities require. Other staff do not have routine access; officers and governors may review relevant records when needed to decide an appeal, respond to legal process, or handle a specific security or abuse matter. We do not treat anything on the Platform as confidential from Library of Code, but we access it only for the purposes described in this policy.

6. Sharing and third parties

We do **not** sell your personal data and do **not** share it with third parties for their own marketing. We do not use third-party analytics or advertising tools on the Platform.

What we run ourselves. The Platform — identity and sign-on, the hosting platform (compute, storage, networking, remote access, and public ingress), and the systems that hold your account records and activity logs — is administered by Library of Code. No external party administers the Platform. Our hosting and storage providers store data on our behalf and may access it only as needed to provide their services or as required by law.

Service providers. A small number of third parties process limited member data on our behalf so we can operate the Platform: the cloud and data-center providers that host our infrastructure in the United States and Finland; an object-storage and DNS provider that holds platform logs, records, and backups of our platform records and serves DNS for our domains; our email and productivity provider; our help-desk / ticketing and status-page provider (Atlassian); our identity-verification provider (Didit), used only when verification is required; an AI-assistance provider (Anthropic), which our staff use to summarize monitoring alerts and help with support and operational tasks and which may therefore receive excerpts of logs or member details that staff include in a request; and Google, which hosts the Workspace accounts we issue. Each processes only what its function requires. The current list, with what each one processes, is published in our **Sub-processor List**, which we update when providers change.

Chat platform. The Platform is accessed and administered through Discord, which processes your data under its own privacy policy and your own account with it, not on our behalf. Discord therefore sees your chat-platform identity, account and resource details shown to you or staff in chat, and your correspondence with staff — but not your hosted content unless you share it in chat.

Disclosure to authorities and others. We may disclose data when we reasonably believe disclosure is required by law or valid legal process, is required to report unlawful content involving minors, or is necessary to protect the safety, rights, or property of Library of Code, our members, or the public. We limit any such disclosure to what is reasonably necessary.

7. Where your data lives

Library of Code is based in the United States, so your data is processed in the US. Our platform infrastructure is hosted in the **United States** (Microsoft Azure) and in **Helsinki, Finland (EU/EEA)** (Hetzner), and data may be transferred between these regions. Platform logs, records, and backups are held in object storage provided by Cloudflare in the United States. Identity-verification data, when verification is required, is processed by Didit in Spain (EU/EEA). Member correspondence, support tickets, chat-platform data, and Google Workspace accounts are handled by Microsoft, Atlassian, Discord, and Google respectively, primarily in the United States; these providers may also process data in other countries under their own terms.

Where our service providers transfer personal data from the EU/EEA or UK to the United States, they rely on the EU–U.S. Data Privacy Framework (and UK Extension) where certified, or on Standard Contractual Clauses (with the UK Addendum) included in their terms. You can request details at it@libraryofcode.org.

8. Retention and deletion

We retain our records for as long as we operate the Platform. Library of Code keeps account and identity records, activity and security logs (including session records), identity-verification results, support correspondence, and our own platform records indefinitely, as part of our operational, security, abuse-prevention, legal, and audit records. We do not run a routine deletion schedule for these records.

Hosted content and issued accounts are the exception. The files, code, and data in a Cloud Services environment exist only while your environment exists: they are deleted when you delete them or when your account or resources are deleted. **We do not back up your hosted environment**; you are responsible for your own backups. A Library of Code Workspace account and its contents are deleted when we close that account. Content captured in session records and logs is retained with those records, not deleted with your environment.

On account deletion: your hosted environments and issued accounts are deleted. Your account records, logs, correspondence, and verification results are retained as described above. If we have suspended or banned you, we keep the records needed to enforce that for as long as the restriction applies.

Your deletion rights still apply. If you ask us to delete your personal data (Section 9), we will delete or anonymize the personal data in our records that we are not required or legitimately entitled to keep — for example, we will keep records needed for an active or reasonably anticipated security, abuse, or legal matter, to enforce a ban, or to meet a legal obligation, and we may keep anonymized or aggregated data that no longer identifies you. We will tell you what we kept and why.

Remember that the Platform itself is provided at our discretion: under the Terms of Service we may delete accounts, Services, resources, or data at any time. This policy governs what happens to *personal data* we hold, not any entitlement to the Platform.

9. Your rights

Depending on where you live, you may have the right to **access**, **correct**, **delete**, or **restrict** the processing of your personal data, to **data portability**, and — where we rely on consent — to **withdraw it**. EU/EEA and UK members have these rights under the GDPR/UK GDPR, and may lodge a complaint with their local data protection authority.

Right to object. Where we process your personal data on the basis of legitimate interests, you have the right to object at any time on grounds relating to your particular situation. We will stop unless we have compelling legitimate grounds that override your interests, rights, and freedoms, or the processing is needed for legal claims.

Contact **it@libraryofcode.org** to exercise a right. We respond within the time required by applicable law (generally one month under GDPR) and may need to verify your identity. Deletion requests are subject to the exceptions in Section 8; we will tell you what we kept and why. We will not delete data in order to avoid a pending request. A request to delete your account data will be treated as a request to close your account.

We honor access and deletion requests from all members, regardless of where they live.

10. Security

We use technical and organizational measures we consider appropriate for a volunteer-run free service, including mandatory single sign-on, authenticated access controls, separation between member environments, restricted staff access, and encryption of data in transit where supported. No system is perfectly secure, and we do not guarantee the security of your data; you remain responsible for your own backups.

11. Children

The Platform is not intended for children under 13, and we do not knowingly collect their data. If we learn we hold data of a child under 13, we will delete it and close the account. Members who are 13 or older but under the age of majority where they live require a parent or guardian's agreement (see the Terms of Service).

12. Changes

We may update this policy. For material changes we will make reasonable efforts to notify members before they take effect and will update the version and date above. If we intend to use your data for a new purpose, we will tell you before we start.

Library of Code, Inc. 30 N Gould St, Ste 21543, Sheridan, WY 82801, USA Email: executive@libraryofcode.org · Privacy requests: it@libraryofcode.org