

Cookie Policy

COLLABOR TECHNOLOGIES LTD

Company number 16888312 | Registered in England and Wales

Last Edited 1 September 2026

1. Who we are and what this Policy covers

COLLABOR TECHNOLOGIES LTD (Collabor, we, us or our) operates the Collabor website and online platform. We are incorporated in England and Wales under company number 16888312. Our registered office is Egerton Mill, 25-27 Egerton Street, Chester, United Kingdom, CH1 3ND.

This Policy explains how we use cookies and similar technologies on collabor.co.uk, Collabor platform subdomains, and other online services that link to it. It should be read with our Privacy Notice. If a third-party website or payment page applies its own technologies, that provider's notice may also apply.

2. Cookies and similar technologies

Cookies are small text files stored by a browser. Similar technologies include local storage, session storage, pixels, tags, software development kits, device or browser signals and other methods that store information on, or access information from, a device.

A technology can be first-party or supplied by another provider, and can last only for a browsing session or remain for a defined period. The legal analysis depends mainly on what the technology does, not simply on whether it is called a cookie.

3. Our legal approach

Under the Privacy and Electronic Communications Regulations 2003, as amended (PECR), storage or access technologies generally require clear information and consent unless a specific exception applies. Where the technology processes personal data, the UK GDPR and Data Protection Act 2018 also apply.

Collabor uses strictly necessary technologies without consent only where they are essential to provide a service requested by the user, transmit communications, authenticate users, protect security, prevent fraud, process a requested payment, record a user's selections, or otherwise fall within a documented statutory exception.

Collabor requests consent before using analytics, marketing and other optional technologies. Consent requires a clear positive action. Continuing to browse, silence, inactivity, pre-ticked controls or accepting general terms does not amount to consent.

4. Categories we use

Strictly necessary. These technologies provide requested functions such as account authentication, security, fraud prevention, consent preference storage and payment processing. They cannot be switched off through the consent manager, although users can use browser controls and may be unable to use the related feature.

Functionality. These remember optional preferences or enable optional features. They are off by default unless a documented PECR exception applies and Collabor provides any required simple objection mechanism.

Analytics. These help us understand visits, navigation and performance so we can improve the service. They are off until the user consents.

Marketing. These would measure campaigns, personalise advertising or track activity across services. Collabor does not currently use marketing cookies. Any future marketing technology will be added to this Policy and will remain off until specific consent is obtained.

5. Technology inventory

The following inventory sets out the technologies used on our website and platform. A conditional entry is used only when the related feature is enabled.

collabor_cookie_preferences - Collabor (first-party cookie)

Category: Strictly necessary

Purpose: Stores the user's category choices, policy or consent-manager version and preference timestamp. It is not used for profiling.

Duration: 180 days; renewed sooner after a material change.

session-id - Collabor-hosted website analytics

Category: Analytics

Purpose: Distinguishes a short website session so page-use and performance events can be analysed.

Duration: 30 minutes. Gated behind Analytics consent.

tsr-scroll-restoration-v1_3 - Collabor / application router (sessionStorage)

Category: Strictly necessary navigation

Purpose: Restores page position and navigation state during the user's current browser session.

Duration: Browser session.

sb-l-auth-token - Collabor / Supabase (localStorage)

Category: Strictly necessary authentication

Purpose: Persists a signed-in session using access and refresh-token information so the user can remain authenticated and access authorised platform functions.

Duration: Until sign-out, session termination, or browser storage is cleared.

Turnstile challenge token and browser signals - Cloudflare

Category: Strictly necessary security

Purpose: Detects automated or abusive traffic and protects registration, login and other sensitive forms. The token is validated server-side.

Duration: Token is single-use and valid for up to 5 minutes.

cf_clearance - Cloudflare (conditional)

Category: Strictly necessary security

Purpose: Stores proof that a Cloudflare challenge was passed, where Turnstile pre-clearance or a Cloudflare challenge feature is enabled.

Duration: Configured Cloudflare Challenge Passage period. Not issued by default Turnstile unless pre-clearance is enabled.

Cloudflare Web Analytics beacon - Cloudflare

Category: Analytics

Purpose: Collects page and performance measurements from browser performance APIs. Cloudflare states that its RUM beacon does not store or access cookies, localStorage, sessionStorage or IndexedDB.

Duration: Current-page, ephemeral browser measurements. Gated behind Analytics consent.

__stripe_mid - Stripe (conditional payment pages)

Category: Strictly necessary payment security

Purpose: Helps Stripe assess fraud risk when a user starts a payment or other Stripe-enabled function.

Duration: Up to 1 year, according to Stripe's current inventory.

__stripe_sid - Stripe (conditional payment pages)

Category: Strictly necessary payment security

Purpose: Short-lived fraud and transaction-risk assessment for Stripe-enabled payment functions.

Duration: 30 minutes, according to Stripe's current inventory.

m, _ab, _mf and related Stripe storage - Stripe (conditional)

Category: Strictly necessary payment security

Purpose: Processes device and activity signals for payment fraud prevention. Exact names vary by Stripe product and configuration.

Duration: Generally session or provider-defined.

Stripe Link authentication and preference storage (conditional)

Category: Strictly necessary when requested

Purpose: Provides a requested Link sign-in or one-click payment experience where the Creator or Brand chooses to use it.

Duration: Varies by Stripe feature.

Future advertising, social tracking or marketing tags

Category: Marketing

Purpose: Collabor does not currently use technology in this category. Any future tool will be named here with its provider, purpose and duration.

Duration: Will not load until Marketing consent is recorded.

6. Stripe and payment technologies

Collabor uses Stripe for payment, fraud-prevention, connected-account and payout functions. Stripe technologies are loaded only on pages or at the point where a user requests a payment-related service, not globally across unrelated pages.

Payment-security and fraud-prevention technologies are treated as strictly necessary where they are proportionate and essential to provide the requested transaction securely. Stripe analytics, advertising or optional Link features are assessed separately. Because Stripe may change its storage names and durations, Collabor reviews the live integration and Stripe's inventory regularly.

7. Your choices

On the first visit, the consent manager offers equally accessible choices to Accept non-essential, Reject non-essential or Customise. Optional categories are off until a choice is made. Rejecting optional technologies does not prevent access to the core website or platform.

A user can reopen Cookie settings from the persistent footer link or settings control and change or withdraw consent at any time. Withdrawal is as easy as acceptance. When consent is withdrawn, Collabor stops the relevant technologies, removes optional first-party identifiers where technically possible and instructs relevant providers to stop consent-based processing where required.

Browser controls can also delete or block storage. Blocking strictly necessary technologies may prevent sign-in, payments, security checks or other requested functions.

8. How long choices last

Your consent preference lasts 180 days. We may ask again sooner if purposes, providers, categories or the consent experience materially change. Storage durations are limited to what is reasonably necessary for the stated purpose.

9. Providers, data and international transfers

Some providers may process device, browser, usage, account, fraud or transaction information as independent controllers or processors. Their own privacy information may apply. Where personal data is transferred outside the UK, Collabor uses an applicable adequacy regulation, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses or another valid safeguard, as described in the Privacy Notice.

10. Contact and complaints

Questions or requests about cookies should be submitted through Collabor's privacy request form or to the privacy contact published in our Legal Centre. Postal correspondence may be sent to COLLABOR TECHNOLOGIES LTD, Egerton Mill, 25-27 Egerton Street, Chester, United Kingdom, CH1 3ND.

Users may also complain to the Information Commissioner's Office or another competent supervisory authority. Details are available through the ICO website.

11. Changes to this Policy

We will update this Policy when technologies, providers, purposes, categories or durations materially change. The public version will show an effective date. We will seek fresh consent before using a new non-essential purpose that is outside the user's previous choice.