

Privacy Notice

How Focus Ladder® collects, uses, shares, protects and retains personal information

Effective date: 10 August 2026

Privacy Summary

- Focus Ladder Ltd, company number 17382413, is the controller.
 - We collect information reasonably needed for payment, billing and location, booking, Sessions, personalised accountability, community administration, Platform operation, security, product improvement, legal compliance, contractual notices and the protection of Members and Company rights.
 - We do not sell identifiable Member data or authorise a provider to use it to train or improve a public or general-purpose AI model for that provider's own purposes. We use reasonable contractual, minimisation and security safeguards, but no online provider can guarantee zero security risk and applicable legal responsibility remains.
- We do not currently use optional analytics, advertising, personalisation or social-media cookies on our own website. Strictly necessary technologies may be used to provide requested website, security, account and payment functions.
- The temporary Signal or WhatsApp community may be closed and replaced by the paid Platform community, Skool or another hosted community service. We may migrate lawful Membership and administration records, but cannot erase copies already stored on another participant's device.
 - Members may exercise applicable UK and, where mandatory law applies, local data-protection rights and may complain to the Information Commissioner's Office or another competent supervisory authority.

1. Controller and Contact

1.1 The controller is Focus Ladder Ltd, company number 17382413, whose registered office is 66 Paul Street, London, EC2A 4NA, United Kingdom (the "Company", "we", "us" or "our"). Privacy, rights and complaint contact: support@focusladder.io.

1.2 The Company was incorporated on 5 August 2026. Business contact, community, Beta and Service-development records previously controlled by Tasleema Kola may be transferred to and continued by the Company where necessary to operate the business, protect rights, manage relationships and communicate with participants. The transfer does not convert historical free participation into a paid contract or remove data-protection rights.

1.3 A later change to the Company's registered name does not create a new controller where the same legal entity and processing continue. We will update the public notice and legal information.

1.4 This Notice should be read with the Focus Ladder® Terms of Service. Capitalised terms not defined in this Notice have the meanings given in those Terms. Contractual ownership or assignment of content does not remove data-protection duties.

2. Scope and Service Development

2.1 This Notice applies to the legal hub, Checkout, payment, booking, official Sessions, Community Sessions where enabled, restricted groups, support, surveys, applications, the Timer Experience, websites, Platform tests, Member-hosting tools and related communications.

2.2 Focus Ladder® is a developing Service. Providers, products, timetables, community tools, Platform features, hosting incentives and processing may evolve. We update this Notice where needed and give additional information before a materially new use where law requires it.

2.3 This Notice is intended to operate consistently with the UK GDPR, Data Protection Act 2018 as amended, Data (Use and Access) Act 2025 and Privacy and Electronic Communications (EC Directive) Regulations 2003, together with applicable international data-protection and privacy law where it applies to the particular processing. It should be read with the Terms of Service and Cookie and Similar Technologies Notice.

3. Information We May Collect

3.1 Identity and contact information: name, email, full billing or contact address, including country, time zone, display name and an 18+ declaration or verification outcome where reasonably necessary.

3.2 Subscription and transaction information from Stripe or another Payment Processor: tier, price, payment status, billing dates, refunds, disputes, chargebacks and limited billing details. We do not normally receive the full card number or security code.

3.3 Membership and operations records: Founding status, Activation Date, bookings, attendance, waiting lists, cancellations, no-shows, community eligibility, access, support, scholarship, warnings, suspension and complaint records.

3.4 Personalised accountability information a Member chooses to share: goals, intentions, task descriptions, deadlines, progress, preferences, check-in notes and continuity patterns reasonably needed for the Service.

3.5 Community and communications information: messages to us; restricted-group messages visible to an administrator account; surveys; Feedback; applications; support; complaints; moderation and security reports.

3.6 Technical, storage, access and security information: browser, device, operating system, IP address or IP-derived region, timestamps, login, access, authentication, strictly necessary cookie or local-storage identifiers, fraud-prevention, error, crash, diagnostic, security and

webhook-delivery records. As at the effective date, the Company does not intentionally deploy optional analytics, advertising, personalisation or social-media cookies on its public legal pages or own Service.

3.7 Platform and Timer Experience interaction information where enabled: timer starts and stops, rounds, agenda or task entries, ladder progression, focus, break and check-in states, completion or celebration states, clicks, feature use, errors and performance information.

3.8 Contract and consent evidence: Terms, Privacy Notice and Cookie Notice versions shown; exact Checkout acceptance text; Customer, account and Stripe identifiers; date and time; checkbox, custom-field or acceptance event; immediate- or delayed-start selection; billing or contact address and country; order confirmation; renewals; cancellations; permissions; email delivery status and related evidential metadata where reasonably necessary.

3.9 Marketing information only where separately permitted: approved testimonial, quotation, image, audio, video, artwork, employer or role, attribution choice, campaign channels and permission record.

3.10 Community Host information where enabled: identity, profile, eligibility, Community Session titles, descriptions, schedules, listings, attendance, complaints, moderation, submitted materials, the main Checkout assignment and acceptance record, the Member-hosting feature-activation record, and any credits, discounts, revenue shares, payments, tax or payout records if incentives are later introduced in the Terms.

3.11 Service-generated metrics and derived information: booking frequency, attendance, utilisation, engagement, plan usage, quality, feature performance and operational analytics.

3.12 Recording information only where a specific recording is notified in advance: audio, video, screen content, display details, moderator notes, access logs, purpose, lawful basis and retention record.

3.13 Cookie and similar-technology information: the categories, providers, purposes and durations listed in the Cookie and Similar Technologies Notice, together with any consent or preference record if optional technologies are introduced.

3.14 Conduct and Safety Evidence. A complaint, witness account, screenshot, message, recording, moderation report or external finding may incidentally contain limited information revealing race or ethnicity, religion or belief, health, disability, political opinion, sexual orientation, sex life, trade-union membership, or an alleged or proven criminal offence. We do not seek a comprehensive criminal record. We collect and retain only what is reasonably necessary to assess safety, contractual conduct, legal claims or enforcement and distinguish allegations from established facts.

4. Sources

4.1 We obtain information from the Member; Stripe or another Payment Processor; booking, Platform, video and community providers, which may include Zoom, Google Meet, Jitsi Meet, Whereby, Signal, WhatsApp, Skool, another hosted community service or replacements; email, CRM, automation, static-site hosting, authentication, support and security providers; analytics providers only if lawfully introduced; Official Facilitators, Community Hosts and authorised contractors; and lawful public or professional sources where reasonably necessary for fraud prevention, legal claims, identity checks, sanctions compliance or business administration.

5. Purposes and Lawful Bases

5.1 Contract: take or arrange payment; save a payment method where expressly authorised; verify and administer billing and account location; record Terms acceptance and any positive start-now request; activate and administer Membership; manage entitlements and bookings, including a temporary manual ledger; deliver official and Community Sessions; operate the Platform and Timer Experience; remember agreed goals; administer the community; provide Contract confirmation on a legally qualifying durable medium; provide support and contractual notices; and administer any hosting credit, discount, referral reward, revenue share or payment introduced by the then-current Terms. An acceptance record alone is not treated as durable-medium delivery unless the Customer can store and reproduce the applicable version unchanged for an adequate period.

5.2 Legal obligation: keep tax, accounting and transaction records; respond to rights requests and complaints; and comply with consumer, court, regulator, tax and other legal duties.

5.3 Legitimate interests, balanced against individual rights: security; fraud and chargeback prevention; confirming billing and account location; maintaining current contact and Service details; conduct enforcement; continuity; quality control; capacity management; operational analytics; product improvement; protecting Focus Ladder® IP, confidential information, chain of title and goodwill; evidence preservation; complaint handling; moderation; serving or responding to legal and contractual notices; and establishing, exercising or defending legal claims.

5.4 Consent where required: optional direct marketing; identifiable testimonials or Showcase publication; non-essential cookies or similar technologies if introduced; a recording where consent is the appropriate basis; intentional storage of special-category information for an optional adjustment or continuity purpose; or a materially new optional use. Consent may be withdrawn without affecting earlier lawful processing.

5.5 Sensitive Conduct Evidence. Where conduct, complaint or safety evidence contains special-category or criminal-offence data, we identify and document an Article 6 basis and any additional Article 9, Article 10, Data Protection Act 2018 Schedule 1 or corresponding applicable-law condition required for the particular purpose. Depending on the facts, this may include explicit consent, legal claims or an applicable substantial-public-interest or unlawful-acts condition. We apply data minimisation, restricted access, accuracy and response safeguards, proportionate retention and any required appropriate policy document or impact assessment.

6. Information Required for the Service

6.1 Name, email, full billing or contact address, including country, payment status, 18+ confirmation and booking information reasonably required to enter into and perform the Contract are necessary. We use the address and country for billing, tax, fraud prevention, account administration, contractual notices, identifying applicable location-related requirements and legal claims. Without required information, we may be unable to activate or administer Membership.

6.2 Most accountability information is voluntary, although declining it may reduce personalised continuity. Detailed profile, phone and business information are optional unless a particular need is explained.

7. Sensitive and Special-Category Information

7.1 The Service is not designed to collect detailed health, disability, race or ethnicity, religion or belief, political opinion, sexual-life, sexual-orientation, biometric or other special-category information. Share only what is necessary and avoid entering it in ordinary Checkout, booking, task or community fields. A statement made during an unrecorded live Session is not routinely converted into a health record by the Company.

7.2 If a Member asks us to record health, disability or other special-category information for an optional reasonable adjustment, access need or personalised continuity purpose, we will provide a separate concise explanation and obtain explicit consent unless another Article 9 condition is documented. The Member may refuse or withdraw that consent. We will record only what is necessary, restrict access and review or delete it when no longer needed.

7.3 A conduct report may necessarily refer to a protected characteristic or an alleged offence in order to describe what happened. We use factual private wording, restrict access, assess reliability and context, give an opportunity to respond where safe and practicable, and do not treat an allegation as a public finding of guilt. A decision is based on evidenced conduct and contractual risk, not protected status.

8. Live Sessions, Restricted Spaces and Recordings

8.1 A display name, image, voice, stated task, message or contribution may be visible to other participants and to the relevant facilitator or Community Host. Members should choose what they disclose. Contract rules prohibit unauthorised recording, stalking, export and disclosure, but information another participant sees may remain on that person's device.

8.2 Focus Ladder® does not record ordinary live Sessions by default and does not covertly record them. A notified recording will explain the purpose, lawful basis, recipients, retention and choices. Automated meeting assistants, transcription tools and AI capture are prohibited unless specifically authorised and lawful.

8.3 A Community Host receives only the participant and booking information made available for the relevant Session. They must use it only to run and moderate that Session, must not build an independent list or use it for marketing, and may be separately responsible for unauthorised processing.

9. Marketing, Showcase Content and Testimonials

9.1 Membership alone does not authorise public use of an identifiable private message, ordinary Session contribution, image, voice, artwork, employer, role or success story.

9.2 Where a Member gives optional Showcase permission and deliberately submits content through the stated route, we use the approved content for the identified channels and attribution choice. The Terms govern the content licence; consent or another lawful basis governs personal-data processing.

9.3 We may use genuinely anonymised and aggregated statistics and de-identified Feedback where no person can reasonably be identified. We do not present fabricated or misleading testimonials.

10. Who Receives Information

10.1 Stripe or another Payment Processor for payment, fraud prevention, refunds, disputes, chargebacks and transaction records.

10.2 The identified Platform, video, booking and community providers, which may include Zoom, Google Meet, Jitsi Meet, Whereby, Signal, WhatsApp, Skool, another hosted community service or replacements identified in joining information or this Notice.

10.3 Website, static-page hosting, email, CRM, automation, storage, authentication, support, IT and security providers acting under appropriate arrangements, and analytics providers only if and after they are lawfully introduced with any required consent controls. The public Legal Hub and landing site must not contain Member lists, private communications, Session content, health information, credentials or confidential source files in static assets. Before a materially new provider receives live Member data, the Company will assess and record the relevant access, contractual and international-transfer safeguards to the extent required by applicable law and proportionate to the processing.

10.4 Official Facilitators, Community Hosts, approved co-hosts and authorised contractors who need limited information for an approved duty and are subject to confidentiality, purpose and access restrictions. An Official Facilitator who receives Member information or restricted access is subject to the confidentiality, purpose, access, safety and data-handling requirements applicable to the role and to any additional role-specific instructions the Company gives. The Company may document the appointment, period, permitted systems and access limits through an Official Facilitator Appointment and Undertaking or an equivalent written or electronic record appropriate to the role.

10.5 Accountants, insurers, solicitors, courts, regulators, tax authorities and law enforcement where necessary for advice, compliance or legal claims.

10.6 A genuine buyer, investor, funder or professional adviser where reasonably necessary for confidential due diligence, financing, restructuring or business transfer, subject to lawful basis, confidentiality, security and appropriate transparency. We do not sell personal information as a standalone list.

11. International Transfers

11.1 Some providers may process information outside the United Kingdom. Where a safeguard is required, we use an adequacy regulation, approved contractual safeguard, binding rules or another lawful mechanism and apply supplementary measures where appropriate.

11.2 A server or data centre being located in the United Kingdom does not by itself rule out remote access, subprocessors, backups, routing or support from another country. Before confidential Member information is placed with a hosting or Platform provider, the Company records the origin region, routine access locations, subprocessors, backups, content-delivery network, transfer mechanism and any available localisation controls. Mere electronic transit through another country is assessed differently from storage or access, but appropriate security remains required.

12. Retention, Migration and Deletion

12.1 We keep information only for as long as reasonably necessary for the purpose, legal obligations, security, complaints, tax and accounting, contract evidence, IP protection and legal claims.

12.2 Indicative periods are: payment, billing-address, tax and accounting records - normally six years after the relevant accounting period; contract, identity, contact-address, acceptance, cancellation and material-dispute records - normally six years after the relationship ends; optional health or adjustment notes - until the adjustment ends or consent is withdrawn, followed by a short evidence period where necessary; routine support and community administration records - normally up to 24 months after closure unless needed longer; security, serious conduct, IP and legal-claim evidence - for the applicable limitation period and while a dispute or enforcement need continues; marketing permissions - while used and for a reasonable evidence period after withdrawal.

12.3 When the temporary Signal, WhatsApp or similar group is replaced by the Platform community, Skool or another hosted community service, we may notify participants and close, delete or archive the official group on the stated migration date, including immediately after the replacement joining route is issued. Eligible paid Members may be invited to the replacement paid community; people who do not become or remain eligible Members do not receive continuing community access.

12.4 We may lawfully migrate or retain our Member and prospect database, including names, contact details, Membership status, consent and Terms records, purchases, attendance, support, moderation, complaints and compliance records. We do not need to retain or import every group message, and we apply purpose limitation, data minimisation and retention rules. Closing the official group cannot erase copies already stored on another participant's device.

12.5 A non-promotional recording, where used, is normally retained no longer than 90 days unless a complaint, legal claim, safeguarding need or specifically authorised training use justifies longer. Community Session listings, assignment evidence and moderation records are normally kept for up to 24 months after hosting access ends, or longer where payment, tax, safeguarding, IP, security or legal-claim reasons require it.

13. Security and Incidents

13.1 We use proportionate technical and organisational measures, including restricted access, authentication, password management, provider due diligence, device security, backups where appropriate, logging and incident response. No online system can guarantee absolute security.

13.2 We assess suspected personal-data breaches and notify the ICO, another competent supervisory authority and affected individuals where and within the period required by applicable law. Members should protect credentials and report suspected unauthorised access promptly.

13.3 Automation and transactional email systems must process only the minimum data needed for payment, consent evidence, activation, Membership, contractual confirmation, access, support and billing events. They must not receive ordinary Session content, Member tasks, health information or other special-category data unless a separate documented need, lawful basis and safeguard exists.

13.4 The Company requires appropriate access controls, secret management, encryption in transit, webhook-signature verification, restricted logs, provider contracts, retention limits and incident procedures. API keys, payment credentials and passwords must not be stored in spreadsheets, source code or ordinary email.

13.5 Public and Confidential Environment Separation. The public Legal Hub and landing page should be a static environment containing only material intended for publication and minimum technical files. Member records, private messages, Session screenshots, health or adjustment information, platform credentials, developer secrets and confidential Focus Ladder® source files must be kept out of that environment and handled only in separately assessed systems with appropriate access controls.

14. Automated Decision-Making and AI

14.1 We do not currently make decisions based solely on automated processing that produce legal or similarly significant effects. The Company does not sell identifiable Member data and does not authorise a provider to use it to train or improve a public, general-purpose or third-party AI model for that provider's own purposes. The Company may use AI-enabled software, coding tools, automation or professional-service systems to build, operate, secure, support, analyse or improve the business and Service where there is a documented lawful basis and, where relevant, an Article 9 condition; the use is necessary and proportionate; data is minimised or redacted; the provider and international-transfer position are assessed; required processor or other contractual terms are in place; and appropriate access, security and retention safeguards apply. Confidential Session content, private Member communications and special-category data are excluded unless a specific documented need and those safeguards exist. No online provider can guarantee zero security risk. This paragraph is not an absolute warranty that a provider cannot suffer unauthorised access or a personal-data breach, and it does not exclude the Company's responsibility under applicable law.

14.2 A future AI feature that materially changes processing will be preceded by updated transparency, an appropriate lawful basis and any required choice, impact assessment or safeguard.

14.3 The Company maintains a proportionate record of material AI-enabled processing and assesses any suspected unauthorised, excessive or sensitive disclosure. Where required and reasonably available, it will seek deletion or restriction, contain the incident, document the risk and notify the ICO or affected people in accordance with applicable law.

15. Adults Only

15.1 Focus Ladder® is intended for adults aged 18 or over. We use a positive 18+ declaration at Checkout and may make a proportionate verification request where a genuine concern arises. We do not knowingly offer Membership to children.

16. Individual Rights

16.1 A person may have the right to access personal information and obtain a copy.

16.2 A person may have the right to correct inaccurate or incomplete information.

16.3 A person may have the right to request erasure where the law applies.

16.4 A person may have the right to restrict processing in certain circumstances.

16.5 A person may have the right to object to processing based on legitimate interests and may object absolutely to direct marketing.

16.6 A person may have the right to receive portable information where the law applies.

16.7 A person may withdraw consent without affecting earlier lawful processing.

16.8 We may need to verify identity and may refuse or limit a request where law permits. We normally respond within one month, subject to lawful extensions. A request provides access to the requester's personal data, not an automatic right to Company IP, trade secrets or another person's information.

16.9 A person outside the United Kingdom may have additional or differently framed rights under mandatory local data-protection law. Where that law applies to the particular processing, we will honour the non-waivable right and applicable response period. Contact us through the same privacy address so the request can be assessed consistently.

17. Complaints, Changes and Contact

17.1 Send a privacy complaint or rights request to support@focusladder.io with enough detail to investigate. We will investigate without undue delay, comply with the statutory response period that applies to the particular right or complaint, and keep the person appropriately informed where practicable. We will not penalise a person for exercising a data-protection right.

17.2 A person may also complain to the Information Commissioner's Office and, where applicable law gives that right, to the competent data-protection or privacy supervisory authority in their country or place of habitual residence, work or alleged infringement. We

review this Notice, the Cookie and Similar Technologies Notice, the Beta, providers, Platform and law as they evolve. We will publish a dated replacement and give additional notice before a material new use where required.