

Privacy Policy

LB TRAINING SOLUTIONS LTD | Company number 17436381

Version 1.0 | Prepared 14 September 2026

1. Who we are

LB TRAINING SOLUTIONS LTD, trading as LB Training, is the controller responsible for the personal information described in this notice.

Registered office: 16 Pasture Avenue, Burringham, Scunthorpe, England, DN17 3NF.

For privacy questions, rights requests or to withdraw consent, email info@lbtrainingsolutions.co.uk or write to our registered office, marked "Privacy request".

2. When this notice applies

This notice covers our website, enquiries, bookings, training administration, student portal, attendance and site sign-in records. While the Coming Soon page is live, it does not collect bookings or create student accounts. The booking and portal sections below apply when those services are available.

If an employer books a course for you, we may receive your name, contact details and course requirements from that employer. We also obtain payment confirmations from Stripe and training records from authorised staff. Please give us accurate information and tell us when it changes.

3. Information we use

Enquiries: your name, email address and information you include in correspondence.

Bookings: your name, email, phone number, date of birth, selected course, booking reference, payment status, receipt link and records of the terms you accepted.

Learning and attendance: your account identifier, teaching dates, attendance status, arrival and departure times, staff notes, and learning activities you mark as complete.

Optional support information: injuries, illnesses, disabilities or adjustments you choose to tell us about. Provide only details relevant to training; do not send detailed medical records through the booking form.

Site visits: staff, contractor or visitor name, role, arrival and departure times. Contractor sign-in also records the company, person or purpose of the visit, and an acknowledgement to report to the contact and check out when leaving.

Technical information: information needed to operate and secure the website, which may include IP address, browser details, requested pages, timestamps and error logs. Logging depends on our server and service settings.

Payments are processed by Stripe. We do not ask you to enter a card number or security code into our booking form, and do not store those details in our booking database.

4. Why we use it

We use booking and contact details to arrange and deliver training, communicate practical information, take payment and provide account access. The usual basis is taking steps at your request before a contract or performing our training contract.

We use information where necessary to meet legal obligations, such as keeping required accounting records. We may use proportionate records for our legitimate interests in operating a reliable training service, managing employer bookings, preventing misuse, resolving complaints and maintaining attendance and site records. We balance those interests against your rights.

Accepting booking terms or reading this notice is not consent to marketing. This website has no marketing sign-up form.

5. Health and support information

Health information is special category data. For optional health details submitted through the booking form, we ask for explicit consent to use them to plan safe participation and appropriate support. Our intended bases for this voluntary collection are consent under Article 6(1)(a) and explicit consent under Article 9(2)(a) of the UK GDPR.

You may leave the optional fields blank and contact us privately about support. You can withdraw consent by emailing us. Withdrawal does not affect use that was lawful before withdrawal. We will explain any effect on support arrangements and consider alternatives. If another legal condition is needed to retain or use particular information, we will explain and document it.

Authorised staff can access support details to arrange and deliver training. Staff should record only relevant information and avoid unnecessary medical details in attendance notes.

6. Student accounts and attendance

After confirmed payment, a new student's initial password is generated by our backend and sent to their booking email through Brevo. A first-time student must choose a new password before accessing course information. Existing account holders keep their existing password. Password reset messages go to the account email.

An emailed initial password is sensitive: protect your email account, change the password promptly and do not share it. The booking database does not contain a plaintext password. Our authentication provider stores a password hash; our email provider processes the message containing the initial password.

Staff record attendance against actual teaching dates. The portal shows the percentage attended so far and the proportion of all scheduled dates attended. These are administrative progress indicators, not an automated qualification decision. Contact us to question or correct an entry.

7. Who receives information

Authorised staff and trainers use information to administer and deliver courses. We use Supabase for authentication and database services, Stripe for payments and receipts, and Brevo for transactional email. Website files are served from our own server using goStatic on Unraid. Necessary technical information is also processed by our network and service providers.

Where required for your course, we may share relevant enrolment, assessment or certification information with the awarding organisation, including Highfield where applicable. For employer bookings we may share appropriate booking and attendance information with the employer; health information is not routinely included.

We may disclose relevant information to advisers, insurers, regulators, law enforcement or other recipients where required by law or necessary to establish or defend legal claims. We do not sell personal information.

8. International processing and security

Service providers may process information outside the UK depending on their service regions and arrangements. Where a restricted transfer applies, we must use a lawful transfer mechanism, such as applicable adequacy arrangements or approved contractual safeguards. Contact us for details of the regions and safeguards applying to your information.

We use access controls to restrict student records, staff-only attendance editing, encrypted connections for account and payment services, and authentication for protected records. Use a unique password and sign out on shared devices. No system can guarantee absolute security.

9. How long information is kept

We keep information only for as long as needed for its purpose and applicable legal or regulatory requirements. Criteria include the training relationship, awarding-organisation requirements, accounting duties, outstanding complaints, legal claims and the sensitivity of the information.

Enquiry records are reviewed when the enquiry is resolved. Booking, payment and training records may need to remain after a course for accounting, certification, audit or dispute purposes. Optional health details should be reviewed when the course and support needs end and removed when no longer necessary. Attendance and visitor records are reviewed against training and site-safety needs. Account and security records are reviewed when access is no longer needed.

We may retain relevant records longer for a specific dispute, investigation or legal obligation. Backup copies may remain until the backup cycle expires and must remain protected. Contact us for the retention period or review criteria applying to a particular record.

10. Your choices and rights

Depending on the circumstances, you can ask to access your information, correct inaccuracies, erase information, restrict its use or receive portable information. These rights are not absolute; some records may be required by law.

You have the right to object to processing based on legitimate interests. You may object to direct marketing at any time. We do not use this website to make solely automated decisions producing legal or similarly significant effects.

Where processing is based on consent, you can withdraw consent at any time. To exercise a right, email info@lbtrainingsolutions.co.uk. We may ask for information to verify your identity. We normally respond within one month; if a permitted extension is necessary, we will explain why.

You can complain to the Information Commissioner's Office at ico.org.uk/make-a-complaint or on 0303 123 1113. You can contact us first so we can try to resolve your concern, but you do not have to do so before contacting the ICO.

11. Cookies, browser storage and external links

The Coming Soon page does not set analytics or advertising cookies and has no tracking scripts. Opening a mail link uses your own email application.

The full portal uses essential browser storage to maintain your sign-in session. Signing out removes the active local session. External checkout, email, content and document services have their own privacy information and may use their own essential technologies. Our full website may request the Supabase client library from jsDelivr; the Coming Soon package has no such request.

If we introduce optional analytics, advertising or similar storage, we will explain it and obtain consent where required before activating it. External learning links may take you to another organisation's website; read that service's privacy notice before submitting information.

12. Updates

We will review this notice when services or use of information changes. The version date appears on the first page. Material changes will be brought to affected people's attention where appropriate.