

WORKPLACEHERO - DATA PROCESSING AGREEMENT

Data processing agreement

Version 1.0 - 25 September 2026 - WorkplaceHero (20 Wenlock Road, London N1 7GU, hello@workplacehero.co.uk).
Download, review and countersign, or use the service under these standing terms.

1. Purpose and parties

This agreement applies where WorkplaceHero processes personal data on behalf of a customer organisation that uses the WorkplaceHero platform, including the CPD log, team dashboard, courses, assessments and 360 feedback. It incorporates the standard contractual terms required by Article 28(3) of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The controller is the customer organisation whose staff and learners use the platform, as identified in the order, account record or countersigned copy of this agreement.

The processor is WorkplaceHero, registered with the Information Commissioner's Office as a data controller (registration number ZB616407). Where an individual uses WorkplaceHero for their own professional development, WorkplaceHero acts as an independent controller of that person's account data, as described in our privacy policy. Nothing in this agreement reduces a learner's own rights over their personal CPD log, which always remains theirs.

2. Subject matter, duration and scope

Item	Detail
Subject matter	The processing of personal data to provide the WorkplaceHero platform and services ordered by the controller.
Duration	For the term of the controller's use of the platform, plus any retention period required by law or by awarding organisation rules.
Nature and purpose	Hosting account records; recording and sharing CPD logs within the organisation's chosen permissions; delivering courses and assessments; issuing certificates; processing payments; providing support.
Categories of data subjects	Staff members, learners, organisation administrators, invitees and other users the controller adds to the platform.
Categories of personal data	Names, work and personal email addresses, job titles, CPD entries and reflections, course and assessment records, certificates, feedback responses, billing and payment records.
Special category data	The platform is not designed to require special category data. The controller must not require staff to enter special category data (for example health information) into free-text fields unless it has a lawful basis and has told WorkplaceHero in writing.

3. Our obligations

WorkplaceHero will: (a) process personal data only on the controller's documented instructions, including for transfers to another country, unless required to do otherwise by UK or EU law - in which case we will tell the controller before processing unless the law forbids it; (b) ensure that everyone authorised to process personal data under this agreement is bound by confidentiality; (c) take the security measures set out in section 5; (d) comply with the conditions in sections 6 to 9 for engaging sub-processors; (e) assist the controller, so far as possible, in responding to requests from data subjects to exercise their rights under UK GDPR and the Data Protection Act 2018; (f) assist the controller in meeting its obligations on security, breach notification, data protection impact assessments and prior consultation; (g) delete or return all personal data when the controller's use

of the platform ends, as set out in section 10; and (h) make available all information needed to demonstrate compliance with this section and allow for, and contribute to, reasonable audits and inspections.

4. Instructions and changes

The controller instructs WorkplaceHero to process personal data to deliver the platform and services it has ordered, in line with our privacy policy and terms. If the controller believes an instruction breaches UK or EU data protection law, we will tell them before carrying it out.

5. Security measures

We take technical and organisational measures appropriate to the risk, including:

- All traffic is encrypted in transit (TLS). The database and stored files are encrypted at rest.
- Course materials, certificates and learner documents are made available only through short-lived signed links.
- Role-based access controls in the application and row-level security in the database mean users can only reach the records their role allows.
- Administrative and staff accounts are protected with multi-factor authentication.
- Continuous backups of the database with point-in-time recovery; a documented incident response process.
- Vulnerability monitoring, dependency updates and least-privilege access for our own staff.
- Sub-processors are bound by written contracts restricting what they may do with personal data.

6. Sub-processors

The controller agrees to the sub-processors listed below. We will give reasonable notice (through our website or by email) before adding or replacing a sub-processor, giving the controller time to object. If the controller objects on reasonable data protection grounds, we will work with them to resolve the concern or, where we cannot, allow them to end the affected service before the change takes effect. Sub-processors are bound by written contracts that give us equivalent obligations to those in this agreement.

Provider	What they do for us	Where
Lovable Cloud (Supabase)	Database, accounts, authentication, file storage	European Union (Ireland region)
Cloudflare	Website delivery from a global edge network	Global edge network
Lovable managed email	Transactional email delivery	European Union
Lovable AI gateway (leading model providers)	In-app assistant and content review	EU / US under Lovable's enterprise terms
Stripe	Card payments and invoicing	EU and US
Klarna	Instalment payment options	EU
Focus Awards	Awarding organisation for regulated qualifications	United Kingdom
Highfield	Delivery of Highfield e-learning courses on its own platform	United Kingdom

7. Personal data breach

We notify affected controllers without undue delay and in any event within 72 hours of becoming aware of a personal data breach affecting their data. The notification sets out, so far as we know it at the time, the nature of the breach, the categories and approximate numbers of data subjects and records concerned, the likely consequences and the measures taken or proposed. We keep the controller informed as the picture becomes clearer.

8. Transfers outside the UK and EU

We store customer data in the European Union and do not move it outside the UK and EU except where a listed sub-processor operates a global network (for example website delivery) or where a specific service requires it. Where personal data is transferred to a country that has not been recognised as adequate, we rely on the International Data Transfer Addendum or the UK/EU standard contractual clauses, together with appropriate safeguards, and we will provide those documents on request.

9. Data subject rights and audits

Where a data subject asks us directly to exercise their rights, we will direct them to the controller where we are acting as its processor, or assist the controller as needed. The controller may, on reasonable notice and no more than once a year (and in case of concern, more often), request information, written confirmations or audit evidence to check our compliance with this agreement; on-site audits by appointment where information requests are not sufficient.

10. Deletion at the end of the contract

When the controller's use of the platform ends, we delete or anonymise the personal data held for that organisation within 30 days, except where UK law or awarding organisation rules require us to keep a record (for example assessment evidence and certificates). Controllers can export their data before leaving, and individual users can delete their own accounts at any time.

11. Liability, term and law

This agreement starts when the controller first uses the platform or countersigns a copy and continues for as long as we process personal data for it. Nothing limits either party's liability for data protection claims except as allowed by law. This agreement is governed by the laws of England and Wales.

12. Signatures

For and on behalf of WorkplaceHero	For and on behalf of the controller
Name:	Name:
Role:	Role:
Date:	Date:
Signature:	Signature:

This document is our standard agreement, version 1.0, published 25 September 2026. Customers who prefer to use their own data processing agreement can email hello@workplacehero.co.uk and we will review it with them.