BeWell IT

Data Processing Agreement

Between BeWell IT Limited and Platform Subscribers

Version 1.6 — 10 September 2026

This Data Processing Agreement ("DPA") forms part of the BeWell Catalyst Platform Agreement ("Agreement") between **BeWell IT Limited**, company number 16095961, registered in England and Wales ("Processor", "we", "our", "us") and the subscribing practitioner, organisation, or institution ("Controller", "you", "your").

This DPA is entered into in accordance with Article 28 of the UK General Data Protection Regulation ("UK GDPR") and supplements the Platform Agreement.

---

1. Scope of This DPA

This DPA governs only the processing of Personal Data where BeWell IT acts as Data Processor on behalf of the Controller. This means End User Personal Data collected through the Controller's courses and programmes on the Platform, as described in Section 2.1 of the Platform Agreement and Section 3.5 of this DPA. It also includes Purchaser Personal Data received by the Processor in connection with the Controller's Course Sales (as defined in Section 2 below), which the Processor processes on the Controller's behalf.

This DPA does not govern:

- BeWell IT's processing of Support Chatbot interactions, where BeWell IT acts as independent Data Controller (see Section 12.5 of this DPA and Section 2.2 of the Platform Agreement);
- BeWell IT's processing of website visitor data, direct-relationship data (including billing and account management), and anonymised, aggregated Platform analytics, where BeWell IT acts as independent Data Controller (see Section 2.3 of the Platform Agreement);
- processing of Purchaser payment data carried out by Stripe in connection with the Controller's Course Sales. Stripe collects and processes that data as the Controller's own payment processor under the Stripe Connected Account Agreement between the Controller and Stripe, not as a sub-processor of BeWell IT (see Section 6.1).

Processing by BeWell IT as an independent Controller is governed by the BeWell IT Privacy Policy, available at bewellit.com/privacy.html.

Data privacy contact: BeWell IT has not appointed a Data Protection Officer under Article 37 UK GDPR. The individual responsible for data privacy matters at BeWell IT is:
Stephan Schoenig, Founder and Principal
privacy@bewellit.com
The Controller may contact this individual for any question or request under this DPA or relating to data protection compliance more generally.

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

Data Protection Officer.

a) BeWell IT has assessed its processing under Article 37(1) UK GDPR. Processing of wellbeing data that may contain health data, and of course questionnaire responses that are intended to contain it, is a core activity; however, at BeWell IT's current scale that processing does not meet the “large scale” threshold, and BeWell IT has therefore not appointed a Data Protection Officer. Stephan Schoenig is the named data privacy contact (Section 1).

b) BeWell IT will keep this assessment under review: at least annually, and promptly upon (i) any material increase in the number of End Users processed on behalf of Controllers, or (ii) the engagement of any regulated-sector subscriber (including NHS bodies and clinical or psychological services).

c) Where the mandatory threshold under Article 37(1) is met, BeWell IT will appoint a Data Protection Officer (which may be on a fractional basis under Article 37(6)) and update this Agreement accordingly.

2. Definitions

Terms not defined in this DPA have the meanings given in the Platform Agreement. In addition:

- **Data Protection Laws**: The UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and any applicable laws relating to the processing of Personal Data;
- **Personal Data**: Any information relating to an identified or identifiable natural person, as defined in the UK GDPR, that is processed by the Processor on behalf of the Controller through the Platform;
- **Processing**: Any operation performed on Personal Data, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction;
- **Data Subject**: An identified or identifiable natural person to whom the Personal Data relates (i.e. your End Users/participants);
- **Sub-processor**: A third party engaged by the Processor to process Personal Data on behalf of the Controller;
- **Personal Data Breach**: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data;
- **Course Sales:** The optional Platform feature described in Section 4.6 of the Platform Agreement, through which the Controller sells places on its courses or programmes to members of the public, with payment taken by direct charge on the Controller's own Stripe Connected Account;
- **Purchaser:** An individual who buys a place on the Controller's course or programme through Course Sales. A Purchaser becomes an End User when they claim their purchase and access the Controller's programme.

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

3. Scope and Purpose of Processing

3.1. Subject Matter

The Processor processes Personal Data on behalf of the Controller to provide the BeWell Catalyst platform services as described in the Platform Agreement.

3.2. Duration

Processing continues for the duration of the Platform Agreement, plus any retention period specified in Section 11 of this DPA.

3.3. Nature and Purpose of Processing

The Processor processes Personal Data for the following purposes:

- Providing Platform access and authentication for End Users;
- Storing and synchronising course/programme data;
- Delivering wellbeing activities, mood tracking, journaling, and progress monitoring;
- Collecting and scoring course questionnaires and surveys administered by the Controller, and making individual and aggregated results available to the Controller;
- Generating analytics and engagement reports for the Controller;
- Providing AI-powered insights (when requested and enabled by the Controller);
- Sending notifications and reminders to End Users on behalf of the Controller;
- Ending an End User's access to a course or programme on the date the Controller sets or, where the Controller sets none, on the Platform default date; sending End Users notices before that date; and, after that date, showing End Users the message and the contact details the Controller has entered for the course;
- Facilitating the Controller's Course Sales: recording purchase entitlements, storing the Purchaser's email address and claim code, sending the Purchaser a claim email on the Controller's behalf, and revoking entitlements where a purchase is refunded;
- Technical support and Platform maintenance.

3.4. Categories of Data Subjects

- End Users enrolled in the Controller's courses or programmes (e.g. students, participants, clients);
- Guest/anonymous users participating without full accounts.
- Purchasers of the Controller's courses or programmes through Course Sales (prospective End Users).
- Individuals whose contact details the Controller enters as the contact for a course (for example the Controller's teachers or staff).

3.5. Types of Personal Data Processed

Category	Examples
Account information	Email address, display name
Authentication data	Hashed passwords, authentication tokens

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

Category	Examples
Wellbeing data	Mood logs, journal entries, activity completion records
Questionnaire responses	Answers to course questionnaires and surveys, including free-text answers, calculated scores, participation status, and date of submission
Pseudonymous respondent identifiers	Randomly generated per-course identifiers under which questionnaire responses are stored, and the mapping between an identifier and the End User's account
Progress data	Course progress, session history, streaks
Enrolment data	Course or programme enrolled in, role, enrolment date, and the date on which the End User's access to the course ends
Course contact details	The email address, telephone number or web address the Controller enters for a course, shown to End Users before and after their access ends
Usage data	App interaction patterns, feature usage
Device data	Device type, OS version, app version
Anonymous IDs	Randomly generated identifiers for guest users
Purchase data	Purchaser email address, purchase claim code, course purchased, Stripe payment reference

In connection with Course Sales, the Processor does not collect, receive, or store payment card details, billing addresses, or Purchaser names. Payment data is collected directly from the Purchaser by Stripe, as described in Section 6.1.

3.6. Special Category Data

The Platform is not primarily designed to process special category data (Article 9 UK GDPR). The Processor acknowledges two distinct routes by which such data may be processed on the Controller's behalf:

- wellbeing data entered by End Users (including mood logs, journal entries, and activity completion records) is reasonably foreseeable to contain health-related information within the meaning of Article 4(15) UK GDPR; and
- where the Controller administers course questionnaires or surveys, the responses are collected for the purpose of measuring wellbeing outcomes and are therefore intended to constitute health-related data, rather than incidentally containing it.

The Processor therefore:

- applies enhanced technical and organisational measures to wellbeing data and questionnaire responses, as set out in Schedule 1, including AES-256 encryption at rest,

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

TLS 1.2+ in transit, organisation-level data isolation, and role-based access control with least-privilege principles;
- stores questionnaire responses under a pseudonymous per-course identifier rather than under the End User's account identifier, as set out in Schedule 1;
- processes such data solely on the documented instructions of the Controller; and
- does not use such data for AI model training or other secondary purposes.

The Controller is responsible for:
- informing End Users, through an appropriate privacy notice, about what data is collected, how it is used, and who processes it;
- identifying the lawful basis under Article 9 UK GDPR on which any special category data processing is based (for example, explicit consent under Article 9(2)(a), or the health or social care basis under Article 9(2)(h) where applicable);
- for UK processing, identifying the relevant condition under Schedule 1 of the Data Protection Act 2018 that accompanies the Article 9 basis, and maintaining an Appropriate Policy Document (APD) under Schedule 1 paragraph 5 DPA 2018 where required (particularly for healthcare organisations and other regulated contexts);
- obtaining any necessary consents from End Users before enrolling them in programmes that may involve special category data processing;
- determining which questionnaires or surveys to administer, and holding any licence or permission required for a standardised instrument it selects;
- carrying out a Data Protection Impact Assessment under Article 35 UK GDPR where required before enabling questionnaires, and acknowledging the Processor's DPIA-support pack within the Platform, which sets out the processing description and the parameters the Controller adopts as its documented instructions; and
- indemnifying the Processor against any claims, losses, or regulatory fines arising from special category data that an End User enters on the Platform in circumstances where the Controller has not complied with the obligations above.

3.7. Deployment to End Users Under 18

Where the Controller deploys the Platform to End Users under the age of 18, the Controller shall:
- comply with all applicable laws relating to the processing of children's Personal Data, including (for UK deployments) the ICO Age Appropriate Design Code ("Children's Code") where applicable;
- implement age verification appropriate to the deployment context, supplementing the Platform's account-creation age declaration where necessary;
- obtain parental or guardian consent where required by law or the Children's Code;
- apply data minimisation, high default privacy settings, and any other relevant Children's Code requirements to its programme design on the Platform; and
- provide End Users with privacy information in language appropriate to their age.

The Controller acknowledges that the ICO Children's Code applies to online services "likely to be accessed by children," and that deployment to under-18 End Users may bring the Controller's processing within its scope.

4. Obligations of the Controller

The Controller shall:

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- Ensure that all processing instructions to the Processor comply with Data Protection Laws;
- Provide End Users with appropriate privacy notices describing the data processing;
- Obtain all necessary consents from End Users before enrolling them in programmes;
- Ensure a lawful basis exists for all Personal Data processing;
- Respond to Data Subject rights requests (with assistance from the Processor as described in Section 8);
- Notify the Processor promptly of any changes to processing instructions;
- Where the Controller enters contact details for a course, ensure that it is entitled to have those details shown to End Users, and keep them up to date;
- Where Course Sales is enabled, provide Purchasers with an appropriate privacy notice, before or at the point of purchase, covering the processing of Purchaser data by the Controller, by Stripe (under the Controller's own agreement with Stripe), and by the Processor under this DPA.

5. Obligations of the Processor

The Processor shall:

5.1. Processing Instructions

- Process Personal Data only on documented instructions from the Controller, unless required by law;
- Inform the Controller if, in the Processor's opinion, an instruction infringes Data Protection Laws.

5.2. Confidentiality

- Ensure that all personnel authorised to process Personal Data are bound by confidentiality obligations;
- Limit access to Personal Data to personnel who need it to perform their duties.

5.3. Security (Article 32 UK GDPR)

Implement and maintain appropriate technical and organisational measures, including:

- **Encryption**: All data encrypted in transit (TLS 1.2+) and at rest (AES-256);
- **Access controls**: Role-based access control with least-privilege principle;
- **Authentication**: Secure authentication through Firebase Auth with support for multi-factor authentication;
- **Infrastructure security**: Hosted on Google Firebase/Google Cloud Platform with SOC 2 Type II certification;
- **Network security**: Firewall rules, DDoS protection provided by Google Cloud;
- **Monitoring**: Automated alerting for suspicious activity and access anomalies;
- **Backup**: Automated daily backups with point-in-time recovery capability;
- **Incident response**: Documented incident response procedures (see Section 9);
- **Tenant isolation**: Multi-tenant architecture with organisation-level data isolation ensuring each Controller's data is logically separated;

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- **Regular review**: Security measures reviewed and updated at least annually.

5.4. Records

- The Processor shall maintain records of processing activities carried out on behalf of the Controller as required by Article 30(2) UK GDPR;
- The Processor shall make these records available to the Controller on reasonable written request, to enable the Controller to meet its own documentation obligations under Data Protection Laws.

6. Sub-processors

6.1. Authorised Sub-processors

The Controller provides general authorisation for the Processor to engage the following sub-processors:

Sub-processor	Purpose	Location
Google Cloud Platform (Firebase)	Infrastructure, hosting, authentication, database, storage	See Data Location below
Google Cloud Platform (Vertex AI, Gemini models)	AI-powered features: Course Chatbot, Support Chatbot, AI Insights, and the content embedding and indexing that powers them (when enabled by Controller)	EU (europe-west1), see Data Location below
Google Workspace (Gmail)	Transactional email delivery on the Controller's behalf (claim emails to Purchasers, notifications to End Users)	Google global infrastructure; transfers safeguarded as described in Section 7
Stripe Payments Europe, Limited	Payment processing, invoicing, and subscription management for the Controller's subscription with BeWell IT (the Controller's direct billing relationship with BeWell IT, outside the scope of this DPA and listed for transparency)	European Economic Area / United Kingdom (Stripe Payments Europe, Limited), with certain support processing by Stripe affiliates including Stripe, Inc. and Stripe, LLC in the United States

Google contractual terms: Processing by Google Cloud Platform, including Firebase and Vertex AI, is governed by the Google Cloud Data Processing Addendum and the Google Cloud Service Specific Terms, which include the Vertex AI data-governance commitments. Under these terms, Google does not use Controller or End User data submitted to Vertex AI, including

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

prompts, inputs, and generated outputs, to train or improve Google's foundation models. Copies of these terms are available to the Controller on request.
Stripe contractual terms: Processing by Stripe is governed by the Stripe Services Agreement and associated Data Processing Addendum (available at stripe.com/legal).
Stripe's role in Course Sales: Where the Controller enables Course Sales, payments are taken by direct charge on the Controller's own Stripe Connected Account under the Controller's direct agreement with Stripe (the Stripe Connected Account Agreement and the Stripe Services Agreement). For that processing, Stripe acts as the Controller's payment processor, not as a sub-processor of BeWell IT, and this DPA does not apply to it. BeWell IT does not transmit Purchaser Personal Data to Stripe: Stripe collects the Purchaser's email address and payment details directly on its hosted checkout page, and BeWell IT receives the Purchaser's email address and payment reference back from Stripe after a successful payment, processing them on the Controller's behalf under this DPA. The Controller is responsible for its own arrangements with Stripe, including accepting Stripe's Data Processing Agreement where applicable and providing Purchasers with appropriate privacy information about Stripe's processing.

Data Location: The Platform operates two infrastructure instances:

- **European instance** (default): Firebase infrastructure (Firestore, Realtime Database, Cloud Functions, Storage) hosted in the EU. AI processing is performed by Google Vertex AI pinned to a European region (europe-west1), ensuring Personal Data processed by AI features remains within the EU;
- **US instance**: Firebase infrastructure hosted in the United States.

Firebase Authentication identity data (such as email address, hashed password, and user identifier) is processed by Google on its global infrastructure and is not hosted on the European instance; such processing relies on the international data transfer mechanisms set out in Section 7.

The standard Platform uses the European instance. Where a custom white-label application is created for the Subscriber, infrastructure may be hosted on either instance depending on the Subscriber's requirements, or on an alternative location at additional cost. The data location is agreed during onboarding and documented in the Subscriber's service configuration.

6.2. Changes to Sub-processors

- The Processor shall notify the Controller at least 30 days before engaging a new sub-processor or replacing an existing one;
- The Controller may object to the change within 14 days of notification, provided that any objection must be on reasonable grounds related to data protection (for example, concerns about the new sub-processor's security measures, data location, or compliance with Data Protection Laws);
- If the Controller objects on reasonable grounds and the parties cannot reach agreement within a further 30 days, the Controller may terminate the Agreement on written notice.

6.3. Sub-processor Obligations

- The Processor shall impose data protection obligations on sub-processors that are no less protective than those in this DPA;

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- The Processor shall be liable to the Controller for the acts and omissions of its sub-processors to the extent that a sub-processor fails to fulfil its data protection obligations, in accordance with Article 28(4) UK GDPR.

7. International Data Transfers

7.1. Transfer Mechanism

Where the Subscriber's data is hosted on the European instance, Personal Data is processed within the EU. Where the Subscriber's data is hosted on the US instance, or where international transfers are otherwise required, such transfers are protected by one or more of the following mechanisms, as appropriate:

- the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, which the Processor shall execute with the Controller on the Controller's written request (templates are available from the ICO and will be made available by the Processor);
- for transfers to US organisations that are certified under the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework (the "UK-US Data Bridge"), where applicable;
- Google's compliance with applicable data transfer frameworks, including the EU-US Data Privacy Framework where applicable;
- technical measures including encryption in transit and at rest.

Course Sales: The Processor does not transfer Purchaser Personal Data to Stripe. Payment data for Course Sales is collected directly from the Purchaser by Stripe under the Controller's own agreement with Stripe, and any international transfers carried out by Stripe (including processing by Stripe, LLC in the United States) are governed by that agreement and by Stripe's own transfer safeguards, including Stripe's certification under the EU-US Data Privacy Framework and its UK Extension, with the EU Standard Contractual Clauses and the UK IDTA or UK Addendum available as fallback mechanisms under Stripe's Data Processing Agreement. Purchaser data received by the Processor from Stripe is processed on the infrastructure instance applicable to the Controller, as described in Section 6.1.

7.2. Transfer Impact Assessment

- The Processor has assessed the laws and practices of the destination countries and concluded that, together with the supplementary measures in place, the transferred data will receive an essentially equivalent level of protection;
- A summary of the Transfer Impact Assessment is available to the Controller on reasonable written request;
- The Processor shall review its transfer mechanisms and Transfer Impact Assessment at least annually, and shall update them promptly if the current basis becomes invalid or if there are material changes in the law or practice of the destination country. No Controller consent is required for such updates, but the Processor shall notify Controllers of any material change.

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

7.3. Cooperation

The Processor shall cooperate with the Controller in completing any data transfer impact assessments required under Data Protection Laws.

8. Data Subject Rights

8.1. Assistance

The Processor shall assist the Controller in responding to Data Subject requests to exercise their rights under Chapter III of the UK GDPR, including:

- Right of access (Article 15);
- Right to rectification (Article 16);
- Right to erasure (Article 17);
- Right to restriction of processing (Article 18);
- Right to data portability (Article 20);
- Right to object (Article 21).

8.2. Notification

- If the Processor receives a request directly from a Data Subject, it shall promptly notify the Controller and shall not respond to the request without the Controller's instructions, unless required by law.

8.3. Self-Service

- End Users can exercise certain rights directly through the Platform (e.g. account deletion, data export via the mobile application's Account settings);
- End Users can withdraw from a course questionnaire at any time, and can choose to have their questionnaire responses deleted at the point of withdrawal;
- The Processor shall maintain these self-service capabilities.

8.4. Response Time

- The Processor shall respond to the Controller's assistance requests within 5 business days.

9. Personal Data Breach

9.1. Notification

- The Processor shall notify the Controller of any Personal Data Breach without undue delay after becoming aware of it, and in any event in sufficient time to allow the Controller to comply with its own obligations under Article 33 UK GDPR (notification to the ICO within **72 hours**)
- Notification shall include, to the extent available:
  - Description of the nature of the breach, including categories and approximate number of Data Subjects and records affected.

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

  - Name and contact details of the Processor's point of contact.
  - Description of the likely consequences of the breach.
  - Description of measures taken or proposed to address the breach and mitigate its effects.
- Where not all information is available within the initial notification timeframe, the Processor shall provide it in phases as it becomes available.

9.2. Cooperation

- The Processor shall cooperate with the Controller in investigating and remediating the breach;
- The Processor shall assist the Controller in meeting its obligations to notify the ICO (within 72 hours) and affected Data Subjects where required.

9.3. Documentation

- The Processor shall document all Personal Data Breaches, including facts, effects, and remedial actions taken, regardless of whether notification to the ICO is required.

10. Audits and Inspections

10.1. Information

- The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and Data Protection Laws.

10.2. Audits

- The Controller may conduct audits of the Processor's data processing activities, subject to:
  - At least 30 days' written notice.
  - No more than one audit per 12-month period (unless required by a supervisory authority or following a Personal Data Breach)
  - Audits conducted during normal business hours.
  - The Controller bearing the costs of the audit.
  - Confidentiality obligations regarding any proprietary information disclosed.

10.3. Alternative

- The Processor may, at its discretion, provide an independent third-party audit report or certification (such as SOC 2 or ISO 27001) to satisfy audit requirements.

11. Data Retention and Deletion

11.1. During the Agreement

- Personal Data is retained for the duration of the Platform Agreement;
- End Users may delete their own accounts and data at any time through the mobile application;

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- The Controller may request deletion of specific End User data at any time.

11.2. Upon Termination

- Upon termination of the Platform Agreement, the Processor shall continue to store the Controller's data for sixty (60) days following termination, during which period the Controller may:
  - export its data through the Platform; or
  - request return of its data in a structured, commonly used and machine-readable format (JSON or CSV)
  - At the Controller's written request made before the end of the 60-day period, the Processor shall extend this period by a further thirty (30) days (up to a total of 90 days)
  - Within thirty (30) days after the end of the applicable retention period, the Processor shall permanently delete all Personal Data and provide written confirmation of deletion upon request.

11.3. Exceptions

- The Processor may retain Personal Data beyond the periods above where required by law.
- The Processor may retain data that has been anonymised in accordance with this clause ("Anonymised Data") beyond the periods above for service improvement, product development, benchmarking, and aggregated analytics. For this purpose:
- "Anonymised" means that the data cannot reasonably be used, whether alone or in combination with other information likely to be available, to identify any individual;
- Anonymisation is applied by removing direct identifiers and by aggregation to a level at which no individual can be singled out;
- The Processor shall review its anonymisation practices at least every three (3) years to confirm that the anonymisation standard remains appropriate having regard to current technology and ICO guidance;
- Anonymised Data is not shared with other Controllers in a form that identifies the source Controller without the Controller's prior written consent.

11.4. Course Sales Purchase Data

- Purchase entitlement records, including the Purchaser's email address and claim code, are retained for as long as the associated entitlement remains active, and are then subject to the retention and deletion rules in Sections 11.1 to 11.3;
- Where a purchase remains unclaimed, the Processor deletes or irreversibly anonymises the Purchaser's email address and claim code twelve (12) months after the date of purchase;
- Claim-email records (containing the Purchaser's email address and claim code) are automatically deleted ninety (90) days after the email is sent.

11.5. Questionnaire Responses

- Questionnaire responses are retained until the End User withdraws and requests their deletion, or until the End User's account is deleted, whichever occurs first, and are otherwise subject to Sections 11.1 to 11.3;

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- Deletion of an End User's account removes that End User's questionnaire responses, including where the End User previously elected to retain them on withdrawal;
- Where the Controller has exported questionnaire responses from the Platform, the exported copy is held by the Controller under its own responsibility and is not deleted by the Processor.

11.6. Course Enrolment Records

Where an End User's access to a course or programme ends, the Processor retains the End User's enrolment record for that course, including the access end date and the End User's activity completion records, for three (3) years after the access end date, so that the Controller can continue to see the End User on the course roster, in exports and in analytics. This retention is carried out on the Controller's documented instruction. The Controller is responsible for its lawful basis, which is expected to be the Controller's legitimate interest in maintaining programme records (Article 6(1)(f) UK GDPR).
At the end of the three-year period the Processor deletes the enrolment record. The record is deleted earlier if the End User deletes their account or the Controller deletes the course.
The End User's own journal entries, practice history and questionnaire responses are not affected by the end of course access and remain subject to Sections 11.1 to 11.3 and 11.5.
The contact details entered for a course belong to the course rather than to an individual teacher's account. Where a teacher's account is deleted, the contact details remain on the course until an administrator of the Controller changes or removes them.

12. AI Processing Addendum

Where the Controller enables AI features on the Platform:

12.1. Scope

The Platform provides two distinct AI features governed by this DPA, each with different data processing characteristics:

a) AI Insights (Practitioner-Facing)

- Processes anonymised, aggregated programme data to generate engagement analytics and recommendations for the Controller;
- Individual End User data is not processed by the AI Insights feature;
- AI Insights are disabled by default and must be actively enabled by the Controller.

b) Course Chatbot (Participant-Facing, Optional Add-On)

- Provides End Users with an AI-powered Q&A assistant trained on the Controller's published course content (Subscriber Content);
- When enabled, individual End User messages (questions) are transmitted to Google Gemini along with relevant Subscriber Content for response generation. This constitutes processing of Personal Data;
- Chat conversations are logged, including the End User's question, the AI response, source references, and any feedback provided;
- The Course Chatbot is disabled by default and must be actively enabled and separately subscribed to by the Controller.

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

The Platform also provides a Support Chatbot, but this is processed by BeWell IT as independent Data Controller and is outside the scope of this DPA. See Section 12.5 below for transparency information.

12.2. Data Minimisation

- **AI Insights**: Only anonymised, aggregated data is used; no individual End User data is processed;
- **Course Chatbot**: Processing is limited to the End User's message, relevant Subscriber Content for context, and the conversation within the current session. No broader End User profile data, wellbeing data, journal entries, or questionnaire responses are included in chatbot processing;
- No use for AI model training: The Processor does not use Controller data, Subscriber Content, or End User data to train AI models, and has confirmed that its AI sub-processor (Google, via Vertex AI) does not use such data to train or improve Google's AI models under the applicable contractual terms referenced in Section 6.1. Should the sub-processor's applicable terms change in a manner inconsistent with this commitment, the Processor shall notify the Controller without undue delay and shall take reasonable steps to maintain the equivalent protection;
- Chat logs are retained for quality monitoring and are subject to the data retention provisions of Section 11.

12.3. Sub-processing

- All AI processing is performed by Google via Vertex AI (Gemini models) as listed in Section 6.1;
- Where the Subscriber's data is hosted on the European instance, Vertex AI is pinned to a European region (europe-west1), ensuring AI processing of Personal Data takes place within the EU;
- The data protection obligations in Google's Cloud Data Processing Addendum and the Google Cloud Service Specific Terms (Vertex AI) apply to all AI processing performed under this DPA. These terms include the no-training commitment referenced in Section 12.2.

12.4. Controller Rights and Responsibilities

- The Controller may disable AI Insights and the Course Chatbot at any time;
- The Controller retains full control over the Course Chatbot's knowledge base, which is derived solely from Subscriber Content the Controller has published;
- The Controller may request deletion of all AI-generated insights and/or Course Chatbot logs;
- AI-generated insights and chatbot responses are not shared with other Controllers or third parties;
- The Controller is responsible for informing End Users that AI features, including the Course Chatbot, are in use within their programme, and for ensuring an appropriate lawful basis exists for the processing of End User messages by the Course Chatbot.
- Lawful basis for Course Chatbot processing: before enabling the Course Chatbot, the Controller shall identify and document an appropriate lawful basis under Article 6 UK GDPR (and, where applicable, Article 9 UK GDPR). In particular:

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- Standard Subscribers (practitioners, coaches, training organisations operating outside regulated health, clinical, or welfare sectors) may rely on legitimate interests (Article 6(1)(f) UK GDPR), provided they complete and retain a documented Legitimate Interests Assessment (LIA) covering the purpose of the processing, necessity, and the balancing test against End User rights and interests;
- Regulated-sector Subscribers (including NHS bodies, clinical psychology services, and higher education welfare services) should obtain explicit opt-in consent from End Users at the point of access, with a clear description of the AI processing and a record of consent retained by the Controller;
- Privacy notice: before enabling the Course Chatbot, all Controllers shall update their privacy notice to End Users to describe (i) what data the Course Chatbot processes, (ii) Google as AI sub-processor, and (iii) the End User's right to opt out of Course Chatbot use.

12.5. Support Chatbot (Transparency Only — BeWell IT acts as independent Controller)

The Support Chatbot is a built-in Platform feature that provides End Users with an AI-powered assistant trained on BeWell IT's own support documentation. BeWell IT processes Support Chatbot interactions as an independent Data Controller, not as Processor on the Controller's behalf, and this processing is therefore outside the scope of this DPA. The BeWell IT Privacy Policy at bewellit.com/privacy.html sets out how BeWell IT processes Support Chatbot interactions.

The Support Chatbot is included here for transparency. The Controller should be aware that:

- the Support Chatbot is a built-in Platform feature that cannot be disabled by the Controller;
- End User messages to the Support Chatbot are transmitted to Google Gemini for processing;
- the Controller should inform its End Users, in its own privacy notice, that the Support Chatbot is a built-in feature whose operator, BeWell IT, acts as independent Data Controller for those interactions.

12.6. AI Accuracy, Automated Decision-Making, and Consent

- AI-generated insights and chatbot responses are provided for informational and educational purposes only. The Processor does not warrant that AI outputs are accurate, complete, or fit for any particular purpose, and the Controller should not rely on AI outputs as a substitute for professional advice. The Processor is not liable for reliance on AI outputs beyond the liability framework in the Platform Agreement;
- The Platform is not designed for, and must not be used by the Controller for, solely automated decision-making that produces legal or similarly significant effects on End Users within the meaning of Article 22 UK GDPR. The Controller is responsible for ensuring that AI outputs are not used in that way;
- The Platform displays an in-app AI consent screen to End Users before they access any AI chatbot feature. This screen requires explicit acknowledgement from the End User and operates as an additional transparency safeguard. The consent screen is not a substitute for the Controller's own lawful basis documentation for Course Chatbot processing;

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

- The Processor will keep its AI processing practices under ongoing review to reflect ICO guidance and, where applicable, equivalent EU guidance on AI and data protection.

13. Liability

- Each party's liability under this DPA is subject to the limitations of liability set out in the Platform Agreement, including the data breach sub-limit in Section 11.3 of the Platform Agreement;
- Nothing in this DPA limits BeWell IT's liability for wilful misconduct or gross negligence, as set out in Section 11.5 of the Platform Agreement;
- The Processor shall indemnify the Controller against losses arising directly from the Processor's breach of this DPA, subject to the liability framework set out in the Platform Agreement.

14. Term and Termination

- This DPA takes effect on the date the Controller subscribes to the Platform and remains in effect for the duration of the Platform Agreement;
- This DPA automatically terminates when the Platform Agreement terminates, subject to the data retention obligations in Section 11;
- Sections 7, 9, 11, and 13 survive termination.

15. Governing Law

- This DPA is governed by the laws of England and Wales;
- Any disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.

16. Amendments

- This DPA may be amended by the Processor to reflect changes in Data Protection Laws, with 60 days' notice to the Controller;
- Material changes require the Controller's consent, which shall not be unreasonably withheld. For the purposes of this clause, a "material change" means a change that reduces the Controller's data protection rights or increases the Controller's obligations under this DPA.

Schedule 1: Technical and Organisational Measures

The following measures are implemented as of the date of this DPA:

Access Control

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

Measure	Description
Authentication	Firebase Auth with email/password, optional MFA
Authorisation	Role-based access control (participant, teacher, admin, platform admin)
Organisation isolation	Firestore security rules enforce organisation-level data boundaries
Session management	Token-based authentication with automatic expiry

Encryption

Measure	Description
In transit	TLS 1.2+ for all connections
At rest	AES-256 encryption on Google Cloud infrastructure
Database	Firestore automatic encryption at rest
Backups	Encrypted backups stored on Google Cloud Storage

Availability and Resilience

Measure	Description
Infrastructure	Google Firebase with multi-region redundancy
Backups	Automated daily backups with 30-day retention
Monitoring	Uptime monitoring with automated alerting
Disaster recovery	Point-in-time recovery capability

Data Minimisation

Measure	Description
Collection	Only data necessary for Platform functionality is collected
Guest access	Anonymous participation available without identifying information

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

Measure	Description
AI Insights	Anonymised, aggregated programme data only; no individual End User data processed
AI Course Chatbot	End User message plus relevant Subscriber Content for current session only; no broader profile, wellbeing, or journal data included
AI training	No Controller data, Subscriber Content, or End User data used to train AI models, including by the AI sub-processor (Google Vertex AI)
Retention	Automatic deletion of inactive guest accounts after 6 months
Questionnaire pseudonymisation	Questionnaire responses stored under a randomly generated per-course identifier; the mapping to the End User's account is held separately and used only to fulfil deletion requests
Questionnaire timestamps	Responses carry the date of submission only, not the time, to reduce the risk of re-identification by correlation
Course access end	Access to course content, community features, reminders and chat is withdrawn on the access end date; only the enrolment record is kept, under Section 11.6

Incident Management

Measure	Description
Detection	Automated monitoring and anomaly detection
Response	Documented incident response procedure
Notification	Controller notified without undue delay after breach detection, in sufficient time for Controller to meet Article 33 UK GDPR obligations
Post-incident	Root cause analysis and remediation documentation

Schedule 2: External Documents Referenced

This Schedule lists the third-party terms, regulatory guidance, and policy documents referenced in this DPA. URLs are current as of the DPA's version date. If a URL changes, the

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom

Processor shall update this Schedule and notify Controllers as part of its ordinary DPA update process under Section 16.

16.1. Sub-processor terms

- Google Cloud Data Processing Addendum: https://cloud.google.com/terms/data-processing-addendum
- Google Cloud Service Specific Terms, including the Vertex AI generative-AI data-governance commitment that Google does not use customer data to train its models: https://cloud.google.com/terms/service-terms
- Vertex AI data governance (summary of the no-training and data-handling commitments): https://cloud.google.com/vertex-ai/generative-ai/docs/data-governance
- Stripe Services Agreement and Data Processing Addendum: https://stripe.com/legal
- Stripe Connected Account Agreement (governing the Controller's own Stripe Connected Account for Course Sales): https://stripe.com/gb/legal/connect-account

16.2. International data transfer mechanisms

- UK International Data Transfer Agreement (IDTA) and UK Addendum to the EU Standard Contractual Clauses (Information Commissioner's Office): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/
- EU-US Data Privacy Framework (US Department of Commerce): https://www.dataprivacyframework.gov/
- UK Extension to the EU-US Data Privacy Framework, also referred to as the UK-US Data Bridge (ICO guidance): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/adequacy-regulations/how-does-the-uk-extension-to-the-eu-us-data-privacy-framework-work/

16.3. UK regulatory guidance

- ICO Age Appropriate Design Code (Children's Code): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

16.4. BeWell IT documents

- BeWell IT Privacy Policy: https://bewellit.com/privacy.html
- BeWell Catalyst Platform Agreement: https://bewellit.com/platform-agreement

BeWell IT Limited – Registered in England and Wales Company No: 16095961
Registered Office: 68 Queens Road, Feltham TW13 5AR, United Kingdom