

EnterpriseJungle, inc. (EnterpriseAlumni) – G-Cloud 15 Terms and Conditions

1) Definitions and Interpretation

In these Terms and Conditions, the following definitions apply:

“Customer” means the public sector body purchasing the Service under the G-Cloud 15 Framework.

“Supplier” means EnterpriseJungle, Inc. trading as EnterpriseAlumni.

“Service” means the EnterpriseAlumni SaaS Platform as described in the Service Definition published on the Digital Marketplace.

“Order” means an agreement or call-off contract entered into under the G-Cloud 15 Framework specifying the Customer’s use of the Service.

“Data Protection Laws” means all applicable laws relating to privacy and data protection, including the UK GDPR, the Data Protection Act 2018 and, where applicable, the EU GDPR.

“Personal Data”, “Controller”, “Processor”, “Processing”, and “Special Category Data” have the meanings given in Data Protection Laws.

“Customer Personal Data” means Personal Data that the Customer (or its authorised users) inputs, uploads, stores, transmits or otherwise makes available through the Service, including Personal Data relating to alumni, community members, or other end users.

“Supplier Account Data” means Personal Data relating to the Customer’s users and contacts processed by the Supplier for account administration, billing, support, security, legal compliance, and relationship management purposes.

“Service Analytics Data” means aggregated and/or de-identified data generated through operation of the Service, including usage metrics, performance statistics, and system telemetry, which does not directly identify individuals.

2) Provision of the Service

1. The Supplier shall provide the Service in accordance with these Terms and Conditions, the Service Definition, and any applicable Order.
2. The Service is provided as a shared, cloud-hosted SaaS platform. The Service is configurable but not bespoke.
3. The Supplier may update the Service from time to time, provided such updates do not materially reduce core functionality.

3) Service Availability and Support

1. The Supplier shall use reasonable endeavours to provide service availability of 99.9% measured monthly, excluding scheduled maintenance.
2. Planned maintenance will be communicated in advance where reasonably practicable.

3. Support is provided via a ticketed service desk during published support hours, with incidents prioritised according to severity.

4) Data Protection and Privacy

1. Allocation of data protection roles

- i) Processor relationship (Customer Personal Data).
Where the Supplier Processes Customer Personal Data in order to provide the Service, the Customer acts as Controller and the Supplier acts as Processor.
- ii) Independent Controller relationship (Supplier Account Data).
The Supplier acts as an independent Controller in respect of Supplier Account Data processed for:
 - account administration and customer support;
 - maintaining accurate, consistent, and up to date supplier and customer account records across the Supplier's systems.
 - billing and contract management;
 - security, fraud prevention, and service integrity;
 - compliance with legal, regulatory, or audit obligations; and
 - establishment, exercise, or defence of legal claims.
- iii) Independent Controller relationship (Service Analytics Data).
The Supplier acts as an independent Controller of Service Analytics Data, provided such data is aggregated and/or de-identified and is used for service management, performance monitoring, capacity planning, security, and product improvement.
- iv) No joint controllership.
Unless expressly agreed in writing, the parties do not act as joint controllers in respect of any Personal Data processed in connection with the Service.

2. Processor obligations (where Supplier acts as Processor)

Where clause 4.1(i) applies, the Supplier shall:

- i) Process Customer Personal Data only on documented instructions from the Customer, unless required by applicable law.
- ii) Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- iii) Ensure that persons authorised to Process Customer Personal Data are subject to confidentiality obligations.
- iv) Not appoint sub-processors without ensuring appropriate contractual protections are in place and maintaining oversight of such sub-processors.
- v) Assist the Customer, taking into account the nature of the Processing, with:
 - responding to data subject rights requests;
 - security incident management and notifications;

- data protection impact assessments and regulatory consultations, where reasonably required.
- vi) At the Customer's option, delete or return Customer Personal Data on termination or expiry of the Order, subject to legal retention requirements.
- vii) A Data Processing Addendum (DPA) shall apply to Processing carried out under clause 4.1(a). In the event of conflict, the DPA shall prevail for data protection matters.

3. Controller obligations (where Supplier acts as independent Controller)

Where the Supplier acts as an independent Controller under clauses 4.1(ii) and/or 4.1(iii):

- i) Each party shall independently comply with its obligations under Data Protection Laws.
- ii) The Supplier shall ensure it has a lawful basis for Processing and shall provide appropriate privacy information where required.
- iii) The Supplier shall not Process Supplier Account Data or Service Analytics Data in a manner incompatible with Data Protection Laws.

4. Customer obligations

The Customer warrants that:

- i) it has all necessary rights, notices, and lawful bases to provide Customer Personal Data to the Supplier;
- ii) it will not provide Special Category Data unless expressly agreed in writing and appropriate safeguards are in place; and
- iii) it remains responsible for determining the purposes and means of Processing Customer Personal Data.

5) Security

1. The Supplier shall maintain appropriate technical and organisational measures designed to protect Personal Data and ensure the confidentiality, integrity, and availability of the Service.
2. Such measures apply:
 - to Customer Personal Data where the Supplier acts as Processor; and
 - to Supplier Account Data and Service Analytics Data where the Supplier acts as an independent Controller.
3. Security certifications and controls are described in the Service Definition.

6) Intellectual Property Rights

1. All intellectual property rights in the Service remain the property of the Supplier.
2. The Customer is granted a non-exclusive, non-transferable right to use the Service for the duration of the Order.
3. No rights are granted other than those expressly set out in these Terms.

7) Customer Data

1. The Customer retains ownership of all Customer Personal Data and other data submitted to the Service.
2. The Supplier shall not access or use Customer Personal Data except as necessary to provide and secure the Service or as otherwise permitted under clause 4.
3. Supplier Account Data and Service Analytics Data are processed in accordance with clause 4.

8) Exit and Data Return

1. Upon termination or expiry of an Order, the Customer may request:
 - i) a copy of its Customer Personal Data in an industry-standard format; or
 - ii) secure deletion of such data.
2. Deletion may be delayed where data is retained in backups or where retention is required by law.

9) Confidentiality

1. Each party shall keep the other party's Confidential Information confidential and use it only for purposes related to the Service.
2. Confidentiality obligations survive termination.

10) Liability

1. Each party's total liability shall be limited to a reasonable and proportionate amount as agreed in the Order.
2. Neither party shall be liable for indirect or consequential losses, except where prohibited by law.

11) Termination

Either party may terminate an Order for material breach subject to reasonable notice and opportunity to remedy.

12) Governing Law

These Terms and Conditions are governed by the laws of England and Wales.