

PAIR – AI Adoption Platform

G-Cloud 15, Lot 2b (Software as a Service)

Service Definition Document

This Service Definition Document describes the PAIR AI Adoption Platform offered under G-Cloud 15, Lot 2b (Software as a Service). It sets out what the Service includes and excludes, how it is delivered and supported, and the responsibilities of PAIR and the Customer.

Pricing for the Service is defined in the PAIR G-Cloud 15 Pricing document. Contract duration and any extension rights are agreed in the Call-Off Order Form. Platform terms apply as set out in the PAIR Platform Terms and Conditions.

Buyer Summary

What is PAIR?

Pair is a web-based AI adoption platform for organisations, focused on delivering role specific AI masterclasses for professionals, and helping organisations drive, track and measure AI adoption.

Who benefits from Pair?

The Masterclasses enable teams to confidently use AI in daily work to achieve measurable productivity gains across key skills every knowledge worker needs such as writing, research, reasoning and automation. Pair's admin dashboard provides leaders with data on AI maturity, adoption, quality impact, and time saved.

The PAIR Hands-on AI Masterclass develops practical AI capability for CoPilot and ChatGPT across three levels: Fundamentals, Proficiency, and Mastery. Each level combines expert-guided instruction and AI-personalised and marked activities that mirror real work. Content is updated monthly to reflect the latest model and tool developments making AI adoption not a one-off effort, but an ongoing company-wide transformation.

About the service

PAIR is a cloud-based AI adoption platform that helps organisations build practical AI capability across their workforce. Users access the service in a web browser (mobile supported) and follow structured AI learning that is personalised to their role. Content includes AI masterclasses, workplace

assignments, and AI-automated feedback on submissions. The platform also includes an in-platform “Showcase” so users can share impactful use cases with colleagues and leadership, plus an admin dashboard to track adoption, progress, and impact metrics (for example, engagement and completion). PAIR updates learning content regularly so programmes stay current as AI tools and ways of working change.

The service is sold as SaaS user licences (“seats”), where each seat is for one named user. Licences are priced per user per year and come in tiers depending on the depth of content and functionality required. PAIR also offers optional rollout components, such as tenant setup (including custom subdomain/branding and SSO integration), launch packages, enablement sessions, and fixed-scope events or reporting, but these are not required to use the core platform.

What is in and out of scope of the offering?

Access to the PAIR adoption platform website is for named/managed users and includes a hosted site, updates, monitoring and standard support. Continuous internet connectivity is required to access the platform, with no offline mode available. Fundamentals and Proficiency can be completed with free ChatGPT or Co-Pilot licences, but for Mastery the paid version is necessary.

What about security and data?

PAIR hosts and processes Customer data in the UK and EEA, with tenant isolation as standard (logical or physical tenancy options). Access to the service is controlled using usernames/passwords with MFA, and administrative access is restricted using role-based access control and least-privilege with regular access reviews. Security assurance includes Cyber Essentials Plus, annual penetration testing via a CHECK provider IT Health Check, and TLS 1.2+ for data in transit. The Customer remains the owner and controller of their data, and PAIR only processes it as needed to deliver and support the Service in line with data protection law.

How does a buyer exit from PAIR?

The Buyer can terminate in line with the Call-Off Contract, including termination for convenience with not less than 90 days’ written notice. Organisation administrators can export learner progress data from the platform in CSV format during the contract. For end-of-contract data extraction, the Buyer submits a request to PAIR. PAIR provides a self-service CSV export tool and will assist with data access and retrieval and provide copies of any personal data processed on the Buyer’s behalf. At the end of the contract, the Buyer’s personal data is securely erased, except aggregated and anonymised data, which may be retained.

Features and benefits

Feature	What it does
Personalisation generation	Creates a bespoke, AI-generated draft of a user's focus areas based on publicly available information about their role and organisation, highlighting areas where AI might benefit them specifically. The learner can then further edit this manually to fine-tune the contents. Aligning skills with organisational goals and operating models.
Personalised activities	Tailors activities and assignments based on user personalisation settings, via use of generative AI. This bridges the gap from theory to real-world application, and improves organisation-wide AI capability through consistent, structured upskilling and feedback loops.
Administration dashboard	Central dashboard for administrators to measure AI maturity, adoption, quality impact, time saved and ROI on AI spend.
Activity submissions	In-platform AI showcase for sharing best-practice outputs with colleagues. Strengthening organisational knowledge-sharing through showcased best practice examples, and enabling leadership to focus on the most impactful org-specific use cases to scale and/or productise.

Scope

PAIR is a public-cloud SaaS service and does not support private cloud, on-premises deployment, or offline use. The Service does not include bespoke software development, custom engineering, or API access. Phone, web chat, and onsite support are not provided; support is delivered via email only. Buyer-owned third-party tool licences (for example, ChatGPT or Copilot) are not included in PAIR licensing. Launch packages, enablement packages, events, and requested data reports are optional add-ons and are not included unless purchased in the Call-Off Order Form. End-of-contract data extraction is not self-service and is provided on request in line with the Data Processing Addendum and contract terms.

Implementation and contractual onboarding

Contractual onboarding starts when the Buyer confirms the Call-Off Order Form, including contract term and the selected licence tier(s), seat volumes, and any optional add-ons. The Buyer also selects the tenant rollout option (Logical Tenant Setup or Physical Tenant Setup) where required. PAIR then runs a short admin onboarding session with the Buyer's nominated point of contact to confirm the agreed setup, admin users, and access approach. Where SSO/IdP integration is in scope for the selected tenant setup, PAIR coordinates the configuration with the Buyer's technical contact using the Buyer's identity provider details. Once tenant configuration and initial admin access are in place,

the Buyer (or PAIR, if agreed) can add named users and issue email invitations so users can create accounts and access the platform via a browser. Service start, billing, and any extension rights follow the Start Date and Contract Period set out in the Call-Off Order Form.

Support

PAIR provides support via email. Support is available 24/7 for critical issues (for example, a platform-wide outage) with an initial response target within 4 hours. Non-urgent requests receive a response within 1 business day (see Appendix A for more information).

Security and data

PAIR is hosted on resilient public cloud infrastructure (predominantly Microsoft Azure, with limited use of Google Cloud Platform for specific services). All long-term storage of Buyer data occurs in the United Kingdom, with some short-term storage and processing occurring in the European Economic Area and other GDPR-compliant processing locations.

PAIR is certified to Cyber Essentials Plus and performs annual penetration testing via an IT Health Check by a CHECK service provider. PAIR is working towards ISO 27001 certification throughout 2026. See Appendix A for a more detailed breakdown of PAIR's security posture.

Availability and resilience

PAIR commits to a 99.9% monthly service availability SLA 99.9% monthly availability SLA (see Appendix A for definition, exclusions, and resilience design).

Exit management

At contract end, the Buyer requests a data export if desired by submitting a request to PAIR Support. PAIR will assist the Buyer with data access and retrieval, including providing copies of any personal data processed on the Buyer's behalf. PAIR confirms the expected turnaround when it receives the request. In addition, standard learner progress exports for organisation administrators are provided as a CSV file via a self-service tool, which is available at any time. At the end of the contract, the Buyer's data is securely erased and there is no additional fee. No post-termination access period is offered in the submitted service listing. The submitted service listing and platform terms do not specify any retention exceptions, other than the Buyer remaining the owner and controller of its

data.

Pricing and Ordering

Pricing model

PAIR is offered under G-Cloud 15, Lot 2b (Software as a Service) using a fixed pricing model. The core platform is licensed on a per user, per annum basis, with different licence tiers providing access to different levels of platform functionality and learning content. Licence prices include ongoing access to the platform, hosting, maintenance, security, and baseline customer success support for the duration of the Call-Off Contract.

One-off and optional services

One-off setup fees may apply at initial rollout to configure the PAIR platform for an organisation. Optional, fixed-scope and time-limited services are available to support rollout, adoption and effective use of the platform. These services are not required to use the PAIR platform.

Contract duration and ordering

Contract duration, licence quantities and any applicable framework discounts are agreed in the Call-Off Order Form in line with G-Cloud framework rules.

Further pricing information

Full pricing details are provided in the Pricing document published alongside this Service Definition on the Digital Marketplace.

Appendix A – Technical service details

Service architecture and hosting

High-level architecture

In-scope (PAIR-managed)

PAIR application (web application and associated backend services).

Core platform services and operational tooling (monitoring, alerting, incident management processes).

Data storage and backup mechanisms used by the service.

Third parties (underlying platforms PAIR uses)

Microsoft Azure (predominant hosting platform; managed services used for compute, storage, identity management, monitoring and logging where applicable).

Google Cloud Platform (GCP) (limited use for specific services).

Software-as-a-service (SaaS) applications used to perform specific storage or processing functions, for example our content management system (CMS).

High-level data flow

End users access the PAIR web application over the public internet.

Application requests are handled by PAIR-managed services hosted in the public cloud.

User data is stored in PAIR-managed data stores in the public cloud (logical separation per buyer/tenant; see tenancy model).

Hosting model

Public cloud hosting

Service hosted predominantly on Microsoft Azure, with limited use of GCP for specific AI services and temporary storage to support those services.

Tenancy model

PAIR operates a hybrid multi-tenant architecture with segregated databases.

For customers opting for a logical segregation model, these databases are hosted on a shared managed database server in the public cloud.

For customers opting for a physical segregation model, these databases are hosted on their own managed database server in the public cloud.

Access to databases is strictly controlled via service principals and allow-lists.

Environments

PAIR operates production and non-production environments with staged testing (unit, integration, staging) as part of the SDLC and change management.

Buyer access is restricted to their own tenant in the production environment.

Data residency and data locations

PAIR hosts all long-term data storage in the UK and maintains a data residency document covering storage and processing, available to interested parties.

Data is stored and processed in full compliance with GDPR.

PAIR benefits from third-party datacentre physical security controls (SSAE-18 / ISAE 3402), implemented by the cloud providers that it uses.

Security controls

Identity and access management

User authentication: is via SSO (via OIDC) or email/password. Multi-Factor Authentication (MFA) is available and is enforced within the PAIR web application for all privileged staff admin accounts.

Administrative access controls to PAIR systems

MFA enforced for management interfaces and administrative actions.

Least-privilege access model.

Role-Based Access Control (RBAC) using Microsoft Entra ID security groups aligned to job roles.

Quarterly access reviews.

Separate dedicated admin accounts for administrative access.

Administrative activity monitored via Azure Activity Logs and Entra ID audit trails.

Personnel Security

Staff with access to personal data are screened to BPSS (Baseline Personnel Security Standard).

Encryption in transit and at rest

Encryption in transit (network)

All network traffic carrying user or sensitive data is protected using TLS. We require TLS 1.2 or later and prefer TLS 1.3 for external client connections (HTTPS / WSS).

Encryption at rest (storage)

Persistent data stored in Azure managed databases and Azure Blob Storage is encrypted at rest using industry-standard symmetric encryption (AES-256 or equivalent). This includes primary data stores, object storage, and managed disks.

Backups, replicas and immutable copies are encrypted at rest under the same standards.

Logging and audit

PAIR maintains incident logging processes and uses platform audit trails (Azure Activity Logs / Entra ID audit trails) for admin monitoring.

Incidents are formally logged with timelines, actions taken, and outcomes, with customer communication where relevant.

Vulnerability management

PAIR performs continuous monitoring and automated scanning across infrastructure and applications.

PAIR utilises automated detection of CVEs in third-party dependencies during development and deployment process (as part of secure SDLC).

PAIR staff ensure timely patching of applications and infrastructure, which is applied based on risk and aligned to industry norms.

Penetration testing

Penetration testing is performed at least annually and scoped to cover the entire web application and underlying cloud infrastructure.

Data sanitisation and deletion

By default, PAIR will securely delete customers' data at the end of contract.

Deletion on request (personal data): PAIR will delete personal data on request (for example, where a user or buyer requests erasure), subject to applicable legal and contractual obligations.

Deletion method (cloud services): Where deletion is requested, PAIR deletes the relevant records/objects from the service. Data is then removed from active systems and, where applicable, becomes unrecoverable from live service components following the normal operation of Azure managed service deletion and lifecycle processes.

Sanitisation / media handling: PAIR does not handle physical media directly for these services. Data sanitisation for underlying storage media is performed by Microsoft as part of Azure's managed service controls (secure decommissioning and sanitisation of retired media).

Availability, resilience, and continuity

Availability target / SLA

PAIR commits to a 99.9% monthly service availability SLA.

If availability falls below 99.9% in a calendar month, customers are eligible for service credits equal to 3% of the monthly fee for each full 1% below the SLA, capped at 15%.

Resilience design

PAIR is designed for resilience using proven public cloud infrastructure and standard platform reliability practices.

PAIR is delivered via managed Platform-as-a-Service (PasS) services across multiple geographic regions, with horizontal autoscaling to handle changes in demand. This layer in turn sits behind a global content delivery network (CDN) and load balancer.

Data resilience includes: multi-region storage replication, regular automated backups and immutable backup copies.

PAIR performs proactive load testing, continuous monitoring, and alerting.

PAIR maintains a documented Business Continuity and Disaster Recovery (BCDR) approach, which is reviewed and exercised.

Incident management

Continuous monitoring and alerting tools are in place to detect degrading performance and potential security events is implemented through a range of services, including Azure App Insights, Azure Monitor and Microsoft Defender for Cloud.

PAIR provides structured major incident communications: Prompt notification to affected customers via email and in-app messaging and regular status updates until resolution.

Major incidents are internally managed through defined escalation, coordination, and incident logging processes.

Support operations

Support channels and support hours

Support issues are raised via email.

Support hours:

Critical incidents will be responded to within 4 hours, 24/7.

Non-critical incidents will be responded to within 1 business day.

Operational monitoring:

The platform benefits from 24/7 automated monitoring.

Integration and technical prerequisites

Browser/device support

Supported devices: Modern desktop and mobile devices (Windows, macOS, iOS, Android, ChromeOS) capable of running a current web browser.

Supported browsers: Current and previous major versions of Microsoft Edge, Google Chrome, Apple Safari, and Mozilla Firefox.

Media/codec prerequisite: To use video features, the browser/device must support a modern video codec such as H.264 (AVC); if codec support is absent or restricted, video playback/recording may be degraded or unavailable.

Client requirements: No native application required; access is via a supported web browser over the public internet.

Network requirements

Requires public internet access to the service.

SSO

SSO is supported via OIDC.

Buyers must provide guest accounts within their IdP to allow testing of the integration to take place.

Buyers must be prepared to take reasonable steps to create app registrations on their IdP, and to share details of these along with required scopes, to facilitate the integration of the SSO connection.

Data export formats

Learner data can be exported as a CSV by administrators of buyer organisations, via a self-serve tool on the administrator dashboard.

Shared responsibility boundaries

PAIR responsibilities

Hosting and operation of the service in public cloud environments.

Secure SDLC practices (peer review, static analysis, testing, IaC, change management).

Platform monitoring, vulnerability scanning, patching based on risk.

Incident response process, major incident communications, and BCDR planning.

Logical tenant segregation controls (as described above).

Staff screening to BPSS and least-privilege admin access controls.

Buyer responsibilities

Managing their own user access policies (who gets access, role assignment within buyer admin scope).

Ensuring end-user device security and appropriate local controls (e.g., device posture, malware protection, secure configuration).

Managing identity provider configuration (if SSO is used) and enforcing MFA policies for their users where applicable.

Ensuring appropriate handling of content/data entered into the platform, according to buyer policy and legal requirements.
