



Terms and Conditions

Pricing

G-Cloud 15 Lot: Lot 2b – Software as a Service (SaaS)

1. Status and precedence

This document provides service-specific information relating to the WiggleDesk solution offered under the G-Cloud 15 Framework.

This document does not override, amend, or replace the G-Cloud Framework Agreement, the Call-Off Contract, or the Order Form.

In the event of any conflict between this document and the G-Cloud Framework Agreement or the Call-Off Contract, the Framework Agreement and Call-Off Contract shall take precedence.

2. Service overview

WiggleDesk is a cloud-hosted workspace and desk management solution designed to support hybrid working, flexible space utilisation, and employee self-service booking of desks and workspaces.

The WiggleDesk software solution is wholly owned by the Bellrock Group and is provided by WIGGLEDESK LIMITED, a Bellrock Group company, which acts as the Supplier under the G-Cloud Framework and any resulting Call-Off Contract.

The service is delivered as Software as a Service (SaaS) and supports browser-based and mobile access to desk booking, workspace availability, and utilisation insights.

WiggleDesk is configurable to reflect the Buyer's organisational structure, locations, and working policies, subject to the scope defined in the Call-Off Order Form.

3. Scope of service

The WiggleDesk service supports a range of workspace and resource management capabilities, which may include (but are not limited to):

- Desk and workspace booking
- External booking of spaces and resources, including meeting rooms and shared facilities, where enabled
- Hybrid working and attendance management
- Location-based availability and capacity views
- Employee self-service booking, amendment, and cancellation
- Workspace and resource utilisation reporting
- Administrative configuration and policy management

The service includes access to a web-based administrative portal to support authorised users to manage:

- User accounts and access permissions

- Desk, space, and resource configuration
- Booking rules, availability, and working policies
- Reporting, dashboards, and notification settings

The service is delivered as a cloud-hosted Software as a Service (SaaS) solution. All primary application hosting and customer data processing are performed within the United Kingdom using Microsoft Azure cloud services.

The WiggleDesk service is delivered directly by the Supplier and does not rely on subcontractors for the provision of the core application service.

The specific features, booking options, and configuration included are defined in the relevant Digital Marketplace service listing and the scope captured in the Call-Off Order Form.

The service does not include bespoke software development, third-party licences, or services outside the agreed scope unless explicitly stated in the Call-Off Contract.

4. Onboarding and mobilisation

Onboarding and mobilisation approach

Successful onboarding is critical to enabling effective use of the WiggleDesk solution and supporting adoption of flexible working practices.

WiggleDesk onboarding is delivered using a structured mobilisation approach designed to establish clear ownership, effective collaboration, and shared understanding of workspace configuration, policies, and ways of working.

The onboarding approach described below sets out how mobilisation is delivered for WiggleDesk services. It is provided to support transparency and consistency of delivery and does not replace or override the G-Cloud Framework Agreement, the Call-Off Contract, or the Order Form.

Supplier onboarding approach

During onboarding, the Supplier:

- Provides an onboarding team and a named delivery lead
- Develops and maintains an onboarding plan aligned to the Buyer's objectives
- Supports configuration of locations, desks, and booking policies
- Provides guidance, training, and onboarding materials
- Uses agreed tools and platforms to support communication and progress tracking
- Identifies and escalates delivery risks where appropriate

Buyer participation and roles

Effective onboarding requires active participation from the Buyer. Onboarding is delivered on the basis that the Buyer identifies appropriate contacts and roles, which may include:

- A Project Sponsor
- A Customer Lead / Workplace Administrator
- Business representatives supporting policy definition

The specific individuals fulfilling these roles are confirmed during mobilisation and reflected in the onboarding plan.

Onboarding activities

Onboarding includes activities such as:

- Confirmation of scope and workspace requirements
- Configuration of desks, locations, and policies
- User access setup
- Training and knowledge transfer
- Go-live readiness and early life support

The sequencing and cadence of onboarding activities are agreed following Call-Off award.

Change management during onboarding

Onboarding is delivered in line with the scope captured in the Call-Off Contract. Any changes or additions to scope are managed through the Call-Off change control process.

Important note

This onboarding approach describes the Supplier's delivery model for WiggleDesk services. All contractual obligations, rights, remedies, and commercial terms are governed solely by the G-Cloud Framework Agreement, the Call-Off Contract, and the Order Form.

5. Service delivery and support approach

The Supplier provides application support services to support the effective operation of the WiggleDesk solution.

The support approach and service targets describe the Supplier's standard support model and are provided for information and transparency only. They do not override or amend the G-Cloud Framework Agreement, the Call-Off Contract, or the Order Form.

Any contractual service levels and remedies are governed solely by the Call-Off Contract.

Support services are provided during standard operating hours as set out in the service listing, with requests raised via agreed support channels.

Access to software updates and enhancements to the licensed solution areas is included as part of the annual subscription, where such updates and enhancements are made generally available.

Support coverage and channels

Support services are provided during the following standard operating hours:

- **Days:** Monday to Friday
- **Hours:** 09:00 to 17:00
- **Exclusions:** England Bank Holidays

Support requests may be raised via:

- Telephone during standard operating hours
- The support portal, available 24/7 (subject to planned maintenance periods)

Support categorisation and response targets

Support requests are prioritised according to severity to support effective triage and resolution.

Severity	Description	Target response time	Target resolution approach
Critical fault	The application is non-operational with no available workaround for business-critical operations, or an issue resulting in data loss.	Within 2 working hours	Resolution targeted within 1 working day
Major fault	Core operations are significantly restricted, though limited business operation remains possible.	Within 2 working hours	Resolution targeted within 2 working days
Important fault	Peripheral functionality is impaired or operating incorrectly, causing inconvenience to non-critical operations.	Within 2 working hours	Addressed in a subsequent planned release
Minor fault	Cosmetic issues, minor errors, or	Within 2 working hours	Considered for a future release

	enhancement requests.		
--	-----------------------	--	--

Availability target

The Supplier operates the WiggleDesk service with a cloud uptime availability target of 99.9%.

Availability targets relate to the core application service and exclude planned maintenance periods.

Software updates and enhancements

Access to software updates and enhancements to the licensed solution areas is included as part of the annual subscription, where such updates and enhancements are made available.

Important note

The support approach, availability targets, and response targets described above represent the Supplier's standard operating model. They do not create contractual guarantees, penalties, or remedies outside those expressly set out in the Call-Off Contract.

6. Security and compliance

Security, hosting, and data protection

The Supplier operates the WiggleDesk service in accordance with recognised information security and data protection standards to support the secure operation of the service.

This section describes the Supplier's standard security, hosting, and governance approach and is provided for information and transparency only. It does not override or amend the G-Cloud Framework Agreement, the Call-Off Contract, or the Order Form.

Hosting and data residency

The service is delivered as a cloud-hosted Software as a Service (SaaS) solution.

All primary application hosting and customer data processing are performed within the United Kingdom and the European Union, using cloud services hosted in UK and EU data centres, including Microsoft Azure and Google Cloud Platform (GCP).

Each Buyer is provided with a logically segregated application environment and associated data store.

Data protection roles

For the purposes of data protection legislation:

- The Buyer acts as **Data Controller**

- The Supplier acts as **Data Processor**

The Buyer is responsible for determining appropriate data classification and for ensuring that the service is used in accordance with applicable data protection and information assurance requirements.

Information security governance

The Supplier operates an information security management framework aligned with recognised standards, including:

- ISO/IEC 27001
- Cyber Essentials and Cyber Essentials Plus

Security governance, policies, and procedures are reviewed and maintained as part of the Supplier's wider information security management system.

Access control and authentication

Access to the service is controlled through role-based access controls and configurable security profiles.

Authentication mechanisms supported by the service include:

- Username and password authentication
- Multi-Factor Authentication (MFA)
- Identity federation with supported identity providers

Administrative access to the service is restricted and protected using enhanced authentication controls.

Data protection in transit and at rest

Data transmitted between the Buyer and the service is protected using TLS encryption (version 1.2 or above).

All customer data stored within the service is encrypted at rest using AES-256 encryption, in line with recognised cloud security principles.

Vulnerability management and testing

The Supplier operates a continuous, risk-based vulnerability management approach as part of its secure development lifecycle (SDLC).

Vulnerability identification, assessment, and remediation activities are embedded within the Supplier's development and release processes and are considered as part of ongoing product development and maintenance planning.

This includes:

- Regular vulnerability scanning

- Independent penetration testing
- Assessment and prioritisation of findings by severity
- Remediation through controlled change management processes

Monitoring and incident management

The Supplier operates centralised security monitoring to support detection of potential security events, including unauthorised access attempts and abnormal activity.

Security incidents are managed through a formal incident management process aligned with recognised standards, including assessment, containment, remediation, and post-incident review.

Secure development and change management

The service is developed and maintained using secure development practices.

Configuration changes and releases are managed through a structured change management process, ensuring that changes are risk-assessed, tested, approved, and auditable.

Data retention and sanitisation

Customer data is retained in accordance with the Call-Off Contract and applicable data protection requirements.

Upon contract expiry or termination, data is sanitised and disposed of using recognised data sanitisation approaches, including cryptographic erasure and secure destruction processes, in line with industry standards.

Integration security

Where integrations with third-party systems are implemented, access is controlled in accordance with the agreed technical design for the integration.

Integration security controls are defined as part of the technical design process and may include the use of APIs, file-based interfaces, secure data exchange mechanisms, or other agreed integration methods, as appropriate to the integration scenario.

Access is restricted to approved functions and data flows and is subject to authentication, authorisation, and access controls designed to protect system integrity.

Important note

Details of the Supplier's security controls, certifications, and technical measures are published on the Digital Marketplace service listing. Contractual security obligations, remedies, and audit rights are governed solely by the G-Cloud Framework Agreement and the Call-Off Contract.

7. Customer responsibilities

Delivery of the WiggleDesk service is based on collaboration between the Supplier and the Buyer.

The service is delivered on the assumption that the Buyer will:

- Appoint appropriate contacts to support onboarding and ongoing service delivery
- Provide timely access to required information for workspace configuration
- Participate in onboarding and review sessions
- Make timely decisions regarding workspace policies and configuration

Where delivery activities are delayed due to dependencies outside the Supplier's control, this may affect delivery timelines and is addressed through the Call-Off change control process.

Important note

This section describes delivery assumptions only. All contractual obligations, remedies, charging mechanisms, and commercial protections are governed solely by the G-Cloud Framework Agreement, the Call-Off Contract, and the Order Form.

8. Dependencies and constraints

Delivery and operation of the WiggleDesk service are dependent on factors outside the Supplier's direct control, including:

- Buyer network connectivity and supported devices
- Availability of identity providers where federated access is used
- Buyer configuration decisions and data inputs

Where dependencies or constraints outside the Supplier's control impact service delivery or timelines, these impacts are addressed through the Call-Off change control process.

9. Change management

Changes to the WiggleDesk service, including changes to scope, configuration, policies, or integrations, are managed through the Call-Off change control process.

No changes are implemented outside the agreed Call-Off change control process.

10. Exit and offboarding

The Supplier operates a standard offboarding process to support Buyer exit at the end of the Call-Off Contract term or following termination.

Under the standard offboarding process, Buyer data is made available in commonly used electronic formats, subject to the scope captured in the Order Form.

The specific offboarding arrangements are confirmed at Call-Off Contract commencement.

Important note

Offboarding arrangements are governed by the Call-Off Contract and the Order Form.

11. Evaluation access and demonstrations

From time to time, and subject to availability, the Supplier may provide access to demonstrations or evaluation instances of the WiggleDesk solution for assessment purposes only.

Any such evaluation access is provided outside the Call-Off Contract, is time-limited and non-entitling, and is not guaranteed.



Make space work.

wiggledesksales@bellrock.co.uk

