

Service Definition – Optimise (Lot 2B: Cloud Software)

Rev 001 @ 18/01/26

Contents

1. Service Overview – What the Service Is.....	2
2. Data Backup, Restore and Disaster Recovery	2
2.1 Data Backup	2
2.2 Data Restore.....	2
2.3 Disaster Recovery.....	2
3. Onboarding and Offboarding Support	2
3.1 Onboarding	2
3.2 Offboarding.....	2
4. Service Constraints.....	3
5. Service Levels	3
5.1 Availability.....	3
5.2 Performance.....	3
5.3 Support Hours	3
6. After-Sales Support	3
7. Technical Requirements.....	3
7.1 Buyer Requirements	3
7.2 Supplier Requirements.....	3
8. Outage and Maintenance Management.....	4
9. Hosting Options and Locations	4
10. Access to Data (Upon Exit)	4
11. Security.....	4

1. Service Overview – What the Service Is

Optimise is a cloud-hosted Software-as-a-Service (SaaS) platform that enables public sector organisations to analyse, model and evidence the sufficiency of education estates.

The service provides secure, browser-based access to data dashboards and analytical tools that support strategic planning, compliance, and decision-making related to school capacity, space utilisation and future demand.

Optimise is delivered as a standardised, multi-tenant SaaS application. All users access the same core platform, with data scoped to their organisation through role-based access controls.

The service is accessed via a modern web browser and does not require any local software installation.

2. Data Backup, Restore and Disaster Recovery

2.1 Data Backup

- All application data is backed up automatically on a scheduled basis.
- Backups are encrypted and stored in geographically resilient cloud storage within the United Kingdom.
- Backup processes are monitored to ensure successful completion and integrity of stored data.

2.2 Data Restore

- Data restoration can be initiated by authorised administrators in the event of data loss, corruption or service failure.
- Restore procedures are documented and periodically tested as part of operational assurance activities.

2.3 Disaster Recovery

- Disaster recovery arrangements are designed to minimise service disruption and data loss.
- Business continuity plans are in place to support recovery following infrastructure failure, cyber incidents or major service outages.

3. Onboarding and Offboarding Support

3.1 Onboarding

- Initial onboarding includes account creation, organisational setup, user provisioning and access configuration.
- Buyers are provided with guidance on platform functionality, data structures and user role management.
- Optional familiarisation or walkthrough sessions may be provided to support effective use of the service.

3.2 Offboarding

- Upon contract termination, access to the service is removed in line with offboarding procedures.
- Buyers may request an export of their data in a commonly used electronic format.
- Data is retained for a defined period to allow secure extraction before permanent deletion in accordance with data retention policies.

4. Service Constraints

- The service is provided as a standardised SaaS platform.
- Customisation is limited to configuration options such as user roles, access permissions and organisational data scope.
- Bespoke software development or modification is not included within the Lot 2B service.
- Planned maintenance windows may be required to deploy updates, apply security patches or perform infrastructure maintenance.

5. Service Levels

5.1 Availability

- The service is designed to be available 24 hours a day, 7 days a week, excluding planned maintenance periods.
- Availability targets are aligned with public sector SaaS expectations.

5.2 Performance

- The platform is designed to support multiple concurrent users without performance degradation under normal operating conditions.
- System performance and availability are monitored to identify and address issues proactively.

5.3 Support Hours

- Support services are available during UK business hours.
- Incidents and service requests are logged, prioritised and managed through defined support processes.

6. After-Sales Support

- After-sales support includes incident management, fault resolution and user support.
- Support requests are triaged and resolved in accordance with agreed service management procedures.
- Platform updates, security patches and enhancements are deployed centrally by the supplier.
- Updates are made available to all users without requiring local installation or configuration.

7. Technical Requirements

7.1 Buyer Requirements

- Users require access to a modern web browser such as Microsoft Edge, Google Chrome or equivalent.
- A stable internet connection capable of accessing secure HTTPS web services is required.

7.2 Supplier Requirements

- No on-premise infrastructure, software installation or specialist hardware is required by the buyer.
- All hosting, infrastructure management, patching and platform maintenance are managed by the supplier.

8. Outage and Maintenance Management

- Planned maintenance activities are scheduled to minimise service disruption.
- Where possible, buyers are notified in advance of planned maintenance windows.
- Unplanned outages are managed through defined incident response and escalation procedures.
- Root cause analysis is undertaken following significant incidents to prevent recurrence.

9. Hosting Options and Locations

- The service is hosted on secure cloud infrastructure.
- All production environments and data storage are located within the United Kingdom.
- Hosting arrangements are designed to meet UK public sector data residency and compliance expectations.

10. Access to Data (Upon Exit)

- Buyers retain full ownership of their data at all times.
- Upon exit, buyers may request a copy of their data in a structured, commonly used electronic format.
- Following the agreed retention period, buyer data is securely deleted in accordance with data handling and disposal policies.

11. Security

- The service follows a defence-in-depth approach to information security.
- Access to the platform is controlled through authentication and role-based access controls.
- Data is encrypted in transit using secure communication protocols and encrypted at rest within the hosting environment.
- Security policies and procedures are aligned with recognised information security management standards.
- Operational security controls support the confidentiality, integrity and availability of buyer data.