



SOPHIA SERVICE DOCUMENT

1. Service Overview

SOPHIA is a cloud-based governance and quality-management platform that centralises organisational policies, procedures, guidelines and Standard Operating Procedures (SOPs). It converts static documents into interactive, structured workflows to improve operational consistency, regulatory compliance and organisational assurance.

The service is designed for regulated sectors including healthcare, higher education, public services, financial services and other environments requiring robust governance and auditability.

SOPHIA provides a single source of truth for governance documentation, combined with role-based access control, workflow automation, analytics, and AI-assisted insights.

2. Service Functionality

2.1 Core Features

- Centralised storage and management of policies, procedures, SOPs and guidelines.
- AI-supported SOP creation and document transformation from uploaded content.
- Version control, audit trail and automated review reminders.
- Workflow automation for drafting, reviewing, approving and publishing documents.
- Interactive SOPs including embedded media, structured steps, decision points and process maps.
- Search, navigation and mobile optimisation for front-line staff.
- Real-time compliance and governance dashboards.
- Cross-site visibility for multi-facility organisations.
- Directory synchronisation for user provisioning and deprovisioning (e.g., Microsoft Entra ID).



- Role-based permissions (viewer, editor, approver, admin).
- Bulk migration capabilities for legacy content and users.

2.2 User Roles

- Team Member: access to policies and processes, interactive SOP navigation, read acknowledgements.
- Team Lead / Editor: create, edit and maintain content, manage approvals (based on user permissions), manage users and teams
- Overview / Governance Role: access to reporting dashboards and compliance analytics.
- Admin: system configuration, manage permissions.

3. Technical Architecture & Requirements

3.1 Hosting

- Hosted in Microsoft Azure UK regions (UK South / UK West).
- Multi-tenant SaaS architecture with strict logical data segregation.
- All data stored and processed within the UK.

3.2 Technical Requirements

Browser-based application, compatible with:

- Microsoft Edge (supported versions)
- Google Chrome (supported versions)
- Safari (supported versions)

Optional integrations:

- Microsoft Entra ID (SSO & directory sync)
- Azure-based services for AI-supported functions
- Optional lightweight signposting integration with Electronic Patient Records (EPRs) where supported

No local installation required.

4. Data Backup, Restore & Disaster Recovery

4.1 Backup

- Automated daily backups of the primary database.
- Incremental backups retained per Azure backup policies.
- All backup data stored within UK Azure regions.



- Encrypted at rest using AES-256.

4.2 Restore

- Point-in-time recovery available within the defined retention window.
- Recovery operations performed through Azure-native mechanisms.
- Customer content can be restored to the most recent valid backup point.

4.3 Disaster Recovery

- Hosted on Microsoft Azure with zone-redundant storage where applicable.
- Platform resilience supported by Azure failover and replication services.
- Recovery Time Objective (RTO): ≤ 4 hours.
- Recovery Point Objective (RPO): ≤ 24 hours.

5. Onboarding & Offboarding

5.1 Onboarding Support

- Initial configuration of organisational structure, permissions and user roles.
- Setup of single sign-on and user directory sync (if required).
- Bulk import of documents and users.
- Administrator training sessions.
- Guidance on governance hierarchy and document categorisation.
- Provision of user guides, SOPHIA SOPs, videos (MP4) and documentation.
- Implementation support including communication plans and engagement workshops.

5.2 Offboarding Support

A structured offboarding process is provided, including:

- Coordinated user access removal
- Export of all customer data in standard formats (PDF, DOCX, CSV)
- Secure encrypted delivery of exported data
- Full review to ensure no active data remains on live systems
- Optional certificate of destruction
- Standard offboarding support included at no extra cost
- Optional enhanced offboarding available if required

6. Service Levels

6.1 Availability

- Guaranteed service availability: 99.9%



- Excludes planned maintenance windows
- Availability measured monthly
- Service credits provided if availability falls below SLA threshold

6.2 Support Hours

- Email and ticketing: Monday–Friday, 09:00–17:00 UK time
- Phone support available during the same hours
- Online ticketing system
- Onsite support available at additional cost

6.3 Support Levels

- Critical issues (e.g., outage, major service failure): target response \leq 4 hours
- High severity: same business day where possible
- Medium/Low severity: resolved based on priority and workload
- Change requests: treated separately, timelines agreed case-by-case
- Enhanced SLA or 24-hour coverage available by separate agreement

7. Service Constraints

- Requires a stable internet connection.
- No installation or local client application required.
- Customisation is limited to configuration (metadata, structure, workflows).
- No support for custom code deployment.
- Advanced process mapping and administration features optimised for desktop interfaces. Some complex workflows may be less suitable for small mobile screens.
- Planned maintenance is notified in advance and performed outside core hours when possible.

8. Outage & Maintenance Management

8.1 Planned Maintenance

- Communicated to customers in advance by email
- Performed outside peak usage hours where possible

8.2 Unplanned Outages

- Email alerts provided
- Managed under SOPHIA's incident response procedure
- Root cause analysis performed for major incidents



9. Security

9.1 Standards & Compliance

Hosted in Microsoft Azure (UK region) with alignment to:

- ISO 27001
- Cyber Essentials
- NHS Data Security & Protection Toolkit (DPST)
- DPIAs and DTAC assessments available on request

9.2 Data Protection

- All data encrypted in transit (TLS 1.2+) and at rest (AES-256).
- UK-only data residency.
- Access controlled through Entra ID or platform-native authentication.

9.3 Access Control

- Username + password
- Multi-Factor Authentication (MFA)
- Identity federation with Microsoft Entra ID or other providers
- Role-based access controls

9.4 Logging & Monitoring

- Full audit trails for all changes.
- Monitoring via Azure-native tools.

10. After-Sales Support & Service Management

- Access to a dedicated support portal for tickets and service requests.
- Named customer success manager (for qualifying contracts).
- Guidance on best-practice usage, document lifecycle management and governance structure.
- Access to ongoing product updates without additional installation.
- Access to user documentation, guides, training videos and SOPs
- Optional onsite training

11. Roadmap (Non-Contractual)

(Roadmap items indicate direction of travel and are not guaranteed deliverables)

- AI chatbot for content navigation.
- Advanced AI-powered governance analyser for identifying gaps, duplication and risk.



- Enhanced training content integration (video generation, guided learning).
- Hierarchical structures for partner organisations.
- Proactive AI-driven suggestions for updating or creating SOPs.
- Automation opportunity identification based on governance documentation.