

Video Sessions for Secure Environments

1. Service Summary

Unilink's Video Sessions service is a cloud-hosted, secure video communication solution designed for use within custodial environments including prisons, secure hospitals, detention centres and secure training institutions. The service enables managed video visits between residents and approved external contacts, providing a controlled alternative or supplement to in-person visits.

The service supports pre-booked, authorised video sessions with identity verification, monitoring and intervention controls equivalent to physical visits. AI-enabled real-time translation and captioning can be used to support communication across language barriers and improve accessibility during video sessions, while maintaining security and staff oversight.

Delivered as a cloud service, Video Sessions provides centrally managed configuration, consistent visiting rules, comprehensive audit and reduced reliance on physical visit infrastructure.

2. Service Features

The service provides a secure, managed video visiting capability, including:

- Secure video sessions between residents and approved external contacts.
- Pre-booking of sessions with time slots defined by the establishment.
- Automated identity verification for visitors during registration.
- Facial recognition to support identity verification during sessions.
- Encrypted peer-to-peer video connections hosted on UK cloud infrastructure.
- Real-time staff monitoring with the ability to intervene or terminate sessions.
- In-call content monitoring to support appropriate use and compliance.
- AI-enabled real-time translation and captions during video sessions.
- Support for social, legal and professional video visits.
- Full audit trail of bookings, participants and session activity.

3. Service Benefits

The service delivers operational, security and wellbeing benefits, including:

- Provides a secure alternative to in-person visits where access is restricted.
- Maintains controlled contact with approved external parties.
- Reduces operational risks associated with physical visits.
- Supports continuity of contact during incidents, restrictions or disruptions.
- Improves communication across languages through real-time translation.
- Ensures consistent application of visiting rules and safeguards.

- Improves oversight of visit activity through monitoring tools.
- Enables visits without travel for approved contacts.
- Provides clear audit trails to support governance and incident review.
- Scales across different custodial environments and operating models.

4. Service Scope

The service covers the management and delivery of secure video sessions between residents and approved external participants.

Residents participate in video sessions only where visits are approved, scheduled and authorised in line with local policy. External participants must be registered and verified prior to participation. Staff oversee booking, monitoring and compliance through staff-facing interfaces.

The service can integrate with visit management, identity and custodial systems where required and supports deployment across multiple establishments through centrally governed configuration.

5. How the Service Works

Video sessions are requested and booked in advance in accordance with establishment visiting rules. Only approved external contacts are permitted to request or attend sessions.

External participants complete registration and identity verification before their first session. During video sessions, facial recognition is used to help verify that the approved individual is participating and remains present throughout the session.

Sessions are delivered using encrypted, browser-based connections and do not require participants to install additional software. Establishments centrally configure session duration, availability, rules and monitoring controls.

Authorised staff can monitor sessions in real time and have the ability to intervene or terminate a session if inappropriate behaviour or policy breaches are identified. All sessions and associated activity are logged to support audit, review and governance.

Where enabled, AI-powered real-time translation and captioning operate during the session to support participants who speak different languages or require accessibility support. Translation features are configurable, operate within the controlled session environment and remain subject to staff oversight.

6. Onboarding and Offboarding

6.1 Onboarding

Onboarding is delivered in a structured manner and typically includes confirmation of service scope, participating establishments, visit types and operating rules.

Configuration includes booking workflows, identity verification settings, monitoring controls, user roles and access permissions. Where required, integrations with visit management or identity systems are implemented and tested.

Pilot deployments can be used to validate workflows and operational fit before wider rollout. Typical onboarding timescales range from 6 to 12 weeks, depending on scope, integrations and operational readiness.

6.2 Offboarding / exit management

Offboarding is managed in a controlled and auditable manner. This includes withdrawal of access, decommissioning of integrations, and handling of retained recordings, data and audit logs in line with contractual and regulatory requirements.

Offboarding activities are typically completed within 4 to 8 weeks, subject to agreed exit arrangements.

7. Support and Service Management

Incidents and service requests are managed in accordance with the agreed contractual service levels and the operational requirements of custodial environments.

Initial response times are:

- High and Medium priority incidents: within 1 hour
- Low priority incidents and general service requests: within 2 hours

Standard support hours are Monday to Friday, 8:00am–5:00pm (UK time). In recognition of the critical nature of custodial systems, High priority incidents are supported 24 hours a day, 365 days a year.

Support is delivered using an ITIL-aligned service management framework. All requests are logged through a central service desk and assessed by a triage function, which assigns priority and routes issues to the appropriate resolver group. Resolution is provided through structured 1st, 2nd and 3rd line support, with clear escalation procedures in place.

Customers are provided with a dedicated Support Portal and an assigned Business Account Manager, who provides ongoing service oversight, technical engagement and escalation support. Service performance and incident trends are reviewed through agreed governance processes.

8. Service Constraints and System Requirements

8.1 Service constraints

- Requires secure network connectivity to support real-time video sessions
- Video quality depends on available bandwidth, device capability and network conditions
- Identity verification and facial recognition depend on camera quality and lighting
- AI-enabled translation and captioning depend on audio quality, supported languages and local policy configuration.

8.2 System requirements

- Approved devices with camera, microphone and supported browser for residents
- Standard PCs or approved staff terminals for operational and administrative users.
- Secure connectivity to the hosting environment (customer cloud or Unilink secure cloud)
- User access and roles managed in accordance with customer security policies.

9. Security and Compliance

The service is designed with privacy and data protection controls built in by design, including role-based access control, audit logging and data minimisation, supporting UK GDPR and relevant information assurance requirements.

Where Unilink provides the managed service, it operates within ISO 27001-certified information security controls, GDPR-compliant data handling practices, and regular external security testing aligned to customer governance.

10. Training

Training is provided to support effective adoption of the self-service platform and is delivered as part of a broader business change approach. Training is role-based and tailored to the needs of different user groups, including system administrators, departmental staff responsible for processing requests, and operational managers with oversight responsibilities.

Training typically covers system configuration, management of self-service modules, workflow and rules setup, request and application processing, reporting and dashboard use, and operational assurance. Training also includes guidance on managing content, responding to resident activity, and using audit and reporting tools to support governance and compliance.

Training can be delivered on-site or remotely, depending on customer preference and operational constraints, and is supported by training materials and user-specific documentation. Where required, training is phased to align with pilot deployments and rollout activities, ensuring staff are prepared ahead of go-live.

Go-live support is provided to assist staff during the initial operational period, helping to address questions, reinforce training and support smooth transition to live service use. This approach supports rapid user adoption and minimises disruption to day-to-day operations.

11. Ordering and Invoicing

This service is ordered via the Digital Marketplace in line with G-Cloud call-off procedures. Pricing is provided separately in the G-Cloud pricing document.

12. Trial Service

A time-limited pilot or proof-of-concept can be provided to validate visit workflows, integrations and assurance policies prior to wider deployment.