

Secure Messaging for Secure Environments

1. Service Summary

Unilink's Secure Messaging service, **eMates**, is a cloud-hosted digital communication platform designed for custodial environments including prisons, secure hospitals, detention centres and secure training institutions. The service enables controlled, auditable messaging between residents, staff and approved external contacts, providing a secure alternative to traditional paper-based correspondence.

eMates operates across both digitally enabled and non-digital prisons, combining secure online messaging, interception and moderation workflows, and controlled paper fulfilment processes. This ensures consistent, safe communication regardless of establishment digital maturity.

Delivered as a centrally managed cloud service, eMates reduces administrative burden, improves communication timeliness and supports consistent application of local communication and security rules.

2. Service Features

The service provides a secure, managed messaging capability, including:

- eMates secure messaging platform for custodial environments
- Secure messaging between residents and approved external contacts
- External messaging via secure web portal and mobile applications
- Intercept and moderation portal for digitally enabled prisons
- Configurable screening of messages and attachments against local rules
- Image attachments supported, subject to moderation and policy controls
- Secure electronic delivery to kiosks and in-room devices
- Controlled paper fulfilment workflows for non-digital prisons
- AI-enabled multilingual translation for messages and replies, where permitted
- Full audit trail of messages, actions and moderation decisions

3. Service Benefits

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

- Faster, more reliable communication than paper-only correspondence
- Supports both digital and non-digital prison environments
- Reduced administrative burden on post room and operational staff
- Consistent interception and moderation of communications
- Improved oversight and traceability of resident messaging
- Reduced risk of prohibited items entering establishments via mail
- Clear audit trails supporting governance and incident review
- Improved multilingual communication for residents and contacts
- Supports safeguarding through structured moderation workflows

4. Service Scope

The service covers the end-to-end management of secure messaging between residents and approved external contacts.

External users submit messages through secure web or mobile channels. Messages are intercepted, screened and moderated in line with local and national policy before being delivered to residents either digitally or through controlled paper fulfilment.

Staff manage interception rules, moderation queues, delivery methods and reporting through secure administrative interfaces. The service supports deployment across single or multiple establishments through centrally governed configuration.

5. How the Service Works

External contacts submit messages through secure online channels, with identity validation, payment checks where applicable, and automated protection against abuse or malicious content.

Messages and attachments are processed through configurable screening and interception rules and reviewed by staff where required. All moderation decisions are recorded.

In digitally enabled prisons, approved messages and attachments are delivered electronically to kiosks or in-room devices. In non-digital prisons, approved messages are securely converted into authorised physical formats and distributed through controlled paper fulfilment workflows.

Prisoner replies are supported in all environments. In digital prisons, replies are created electronically and moderated before release. In non-digital prisons, handwritten or typed replies are securely captured, moderated and returned digitally to external recipients.

All activity is logged centrally, providing full traceability across submission, moderation, delivery and reply.

6. Onboarding and Offboarding

6.1 Onboarding

Onboarding is delivered as a structured process including confirmation of scope, establishments, interception rules, moderation workflows and delivery models. Configuration supports both digital delivery and paper fulfilment options.

Typical onboarding timescales range from three to 12 weeks, depending on scale and configuration

6.2 Offboarding / exit management

Offboarding is managed in a controlled and auditable manner, including withdrawal of access, decommissioning of integrations and handling of retained message data in line with contractual and regulatory requirements.

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

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

- Message interception and moderation rules are subject to local policy and regulation.
- Availability of attachments and translation features depends on configuration.
- Delivery method depends on establishment digital capability and access rules.

8.2 System requirements

- Standard PCs or approved terminals with a supported web browser for staff use.
- Secure web access for external contacts via browser or mobile application.
- Secure network connectivity to the hosting environment.
- Role-based access controls aligned to customer security policies.
- Printing infrastructure for paper fulfilment

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 for operational and administrative staff covering use of the intercept portal, moderation workflows, exception handling, paper fulfilment processes, reporting and audit. Training can be delivered remotely or on-site and aligned with rollout and go-live activities.

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 interception workflows, digital and paper delivery models, and operational fit prior to wider deployment.