
Phonehub IO Ltd

Prison Email

G-Cloud 15 Service Definition Document

Supplier

Phonehub IO Ltd

Registered Office

1-2 The Old Church, St. Matthews Road,
Norwich, England, NR1 1SP

Registered in England and Wales.

Company Number

9568821

Framework

G-Cloud 15

Last Updated

07 January 2026



Crown
Commercial
Service
Supplier



Contents

Introduction	3
What the service is	3
Features	3
Data backup and restore, and disaster recovery	4
Business continuity and disaster recovery plans	4
Onboarding and offboarding	4
Onboarding	4
Offboarding	4
Service constraints	4
Service levels	5
Compensation if service levels are not met	5
After-sales support	5
Technical requirements	5
Outage and maintenance management	5
Hosting options and locations	5

Introduction

What the service is

Prison Email is a secure end-to-end encrypted emailing service purpose built to improve communication channels between prisoners, patients, and the outside world whilst ensuring that all communications remain identity-verified, secure, and auditable. The service incorporates communication monitoring with safeguarding, regulatory, and security policies to aid in the early identification of negative behaviours, trends, and communication patterns that may indicate safeguarding or security risks.

Features

Identity-verified recipient accounts

Secure and automatic ID verification for external participants to verify email recipients and maximise safeguarding by ensuring that children are registered in advance using a simple selfie (Prison staff have the ability to request additional ID for children where required for public protection purposes).

Automatic content scanning

Prison Email offers intelligent communication monitoring with advanced AI-powered features such as pattern analysis, word-level analysis, and word-level classification to detect behaviours, trends, and repeating communication structures that may indicate a risk. This could aid in the identification of bullying, coercion, coded communication, extremist rhetoric, radicalisation, sudden communication changes (e.g., frequency drops or unusual wording that could indicate manipulation or exploitation) mental health declines or self-harm risks to support early intervention.

Automatic attachments scanning and blocking of policy-violating content

Prison Email can automatically scan photo attachments and identify cases of indecent imagery, or nudity and block policy-violating content.

Flexible configurations, policy enforcement and access revocation

The service can be configured and scaled to each establishment's needs and altered to meet any future policy changes at the request of the buyer. Staff retain full operational oversight and possess the ability to revoke access from users in the event of a policy or rule breach.

Configurable retention and deletion policies

All communications are recorded, according to policy and instantly retrievable. Recordings are retained according to strict retention processes, ensuring that establishments comply with policy requirement. Access to communications is restricted, controlled, and audited through an intelligent and secure user interface.

Administrative dashboard for reviewing activity and managing access

Detailed and salient data can be extracted directly from the monitoring interface that can be used to identify areas requiring support, evaluate feedback for continuous improvement, or for billing purposes.

End-to-end encrypted sending and receiving of emails

End-to-end encryption ensures that all messages are encrypted from the moment they are sent until they are opened by the authorised recipient, preventing interception, tampering, or unauthorised access at any point in transmission.

Data backup and restore, and disaster recovery

Business continuity and disaster recovery plans

Phonehub IO Ltd uses triple redundancy to ensure that services remain operational, even in the unlikely event of a datacentre failure. All data is stored triple mirrored in zone redundant storage across three separate datacentres making the service resilient to the failure to two data centre failures.

Our disaster recovery plans form part of our ISO 27001 information security management system.

The service is fully backed up so that in the event of a complete disaster all service can be readily restored to full operation.

Onboarding and offboarding

Onboarding

The Phonehub IO Ltd team will work closely with the buyer's team to complete onboarding process. For cloud only installations, establishments need only facilitate access to our service from web browsers to get up and running. Deployment of new establishments is a simple configuration and does not require any on-site visits by our staff, but where this is preferred we are happy to provide on-site support.

Further support for onboarding such as in-person and/or remote training will be provided where appropriate and upon request. Full documentation will also be provided in PDF format, along with video guides.

Offboarding

Data owned by the buyer will remain available for downloadable for a period of 90 days through the management portal. Recordings and communications records will be retained for interception purposes by Phonehub IO Ltd according to the agreed standard retention policy.

Service constraints

Access to the service is only available from pre-approved networks, approved networks may be updated at any time through agreed communications channels.

Service levels

Services are available 24/7, 365 with guaranteed SLA of 99.9% of availability.

Compensation if service levels are not met

Financial compensation will be calculated based on the length of time the service is unavailable compared to the expected availability as a proportion of the regular fees paid by the buyer.

After-sales support

Phonehub IO Ltd provides continual after sales support during business hours at no additional charge.

Technical requirements

The minimum access requirement for a prisoner or staff member is a Chromium based web browser such as Microsoft Edge.

For prisoners Android Tablets flashed with the Hydrax Operating system are supported. Devices must be compatible with the Android Open Source Project

Outage and maintenance management

While the service remains accessible 24/7, 365 individual features of the service may occasionally be unavailable for routine maintenance. So far as practicable, maintenance work will be carried out during non-working hours, where this is not possible, every effort will be made to notify the buyer in advance.

The service implements rolling updates so the majority of maintenance work will have no impact on service availability.

Hosting options and locations

This is a managed service; customers are able to specify the region that they require their data to be held in subject to the availability of suitable cloud resources.

For example for UK government customers data is stored in England where as for Australian jurisdictions data is stored in New South Wales.