

Justice and Public Safety Information Sharing Services – Service Definitions

This document defines three related G-Cloud services designed for policing, justice, prisons, ROCUs and government arm's-length bodies. The services focus on secure information sharing, coordination and visibility, not intelligence analysis or decision-making.

1. Justice and Public Safety Intelligence Sharing Services

Service summary

This service enables secure, auditable information sharing between police forces, prisons, ROCUs and justice partners. It improves visibility of relevant information across organisations, reducing delays, duplication and reliance on informal channels while supporting lawful, controlled access to sensitive data.

Key features

- Secure information sharing across justice partners
- Role-based access and permissions
- Case-linked information visibility
- Audit trails and access logging
- Integration with policing and prison systems
- Configurable data sharing rules
- Scalable cross-agency architecture

Key benefits

- Faster access to relevant information
- Reduced reliance on email and spreadsheets
- Improved coordination across agencies
- Stronger audit and compliance controls
- Reduced operational risk
- Better oversight for senior leaders

Service definition

This service provides the design, implementation and support of secure information-sharing capabilities across justice and public safety organisations. It focuses on enabling authorised users to access and share relevant information in a controlled, auditable way. The service does not provide intelligence analysis, assessment or operational decision-making.

2. Multi-Agency Case Coordination and Information Sharing Services

Service summary

This service supports coordinated case working across multiple agencies involved in public safety and justice. It provides shared visibility, structured workflows and consistent updates to improve collaboration across police, prisons, probation, ROCUs and partner bodies.

Key features

- Shared multi-agency case views
- Workflow and task coordination
- Secure updates and notifications
- Partner-specific access controls
- Integration with existing case systems
- Audit trails and reporting
- Escalation and handover controls

Key benefits

- Improved coordination on complex cases
- Reduced duplication of effort
- Clear ownership and accountability
- Fewer delays caused by information gaps
- Better experience for frontline teams
- Improved governance and oversight

Service definition

This service provides tools and integration to support coordinated case management and information sharing across multiple justice and public safety organisations. It enables shared visibility and communication while maintaining clear boundaries, permissions and accountability. The service does not replace existing case systems or make operational decisions.

3. Prison–Police Information Exchange Services

Service summary

This service improves information exchange between prisons and police forces by providing secure, structured and auditable channels for sharing relevant updates. It reduces delays, missed information and manual work caused by fragmented communication methods.

Key features

- Secure prison–police information exchange

- Case and individual-linked updates
- Controlled access for authorised users
- Integration with prison and policing systems
- Automated notifications and updates
- Audit logging and compliance reporting

Key benefits

- Timelier sharing of relevant information
- Reduced manual communication effort
- Improved risk awareness and coordination
- Stronger governance and auditability
- Reduced reliance on informal channels
- Better joint working between prisons and police

Service definition

This service provides secure, integrated capabilities to support information exchange between prisons and police forces. It enables authorised sharing of relevant updates and information while maintaining strong access controls and audit trails. The service does not perform risk assessment, intelligence analysis or decision-making.

Common delivery, security and governance

Delivery approach

Services are delivered using a phased, collaborative approach including discovery, design, integration, configuration, testing, deployment and enablement. Delivery is iterative and designed to minimise disruption.

Security and compliance

All services operate within an ISO/IEC 27001 certified Information Security Management System and are supported by Cyber Essentials Plus. Controls include role-based access, monitoring, incident management and change control. UK-based, security-cleared staff are available where required.

Data handling

All data is processed in accordance with contractual requirements and applicable UK data protection legislation. Access is restricted, logged and auditable.

Service boundaries

These services enable information sharing and coordination only. They do not provide intelligence analysis, prediction, risk scoring, or operational or legal decision-making. Responsibility for decisions remains with the customer.