

Interoperability Handbook

ABSTRACT

The intent of this document is to provide an overview of interoperability, support data sharing within the policing IT landscape and to promote the integration of policing and wider law enforcement systems.

DATE:	17 July 2026
VERSION:	1.1
DOCUMENT REFERENCE:	

COPYRIGHT:	
NUMBER OF PAGES:	38
CLASSIFICATION:	OFFICIAL

Contents

Introduction	4
Context.....	4
Audience	5
Scope	6
Why Interoperability matters	7
What is interoperability?.....	9
Interoperability Definition	10
Interoperability in policing. Example	11
What Does an Interoperable System look like?.....	11
Interoperability Maturity Assessment	13
Planning for Interoperability.....	19
Interoperability and Suppliers.....	22
Assessing a supplier's level of interoperability	23
Interoperability Resources.....	24
Foundational Interoperability Resources	24
Structural Interoperability Resources	25
Semantic Interoperability Resources	28
Organisational Interoperability Resources.....	29
Interoperability Strategy	30
The National Policing Digital Strategy.....	30
Interoperability and Policing Stakeholders	31

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Interoperability reference table	33
Review	34
Document Information.....	34
Version History	34
Consultation.....	34
Approvals	36
Distribution List.....	36
Core Principles Summary	37

DATE:	17 July 2026
VERSION:	1.0
DOCUMENT REFERENCE:	

COPYRIGHT:	
NUMBER OF PAGES:	38
CLASSIFICATION:	OFFICIAL

Introduction

Context

Across policing, we have long recognised the need to improve how our systems connect, how our data flows and how our organisations collaborate digitally. The case has been made repeatedly through the NPCC Policing Vision 2030, the National Policing Digital Strategy 2025–2030 and the Police Productivity Review, the Strategic Policing Requirement and the National Police IT Reform Strategy. Interoperability has been consistently identified as a national priority.

However, in the context of the Reform White Paper, interoperability moves from ambition to structural enabler.

The reform programme sets out a transition from 43 largely fragmented forces towards a coherent national system, including the creation of a National Police Service. It seeks consistent national standards, data-driven performance management, productivity reform, AI deployment, strengthened digital crime capability and long-term financial sustainability.

None of this can be delivered without interoperable digital foundations.

Interoperability underpins our ability to:

- Share data seamlessly across force and organisational boundaries
- Implement national platforms and standards
- Enable AI and advanced analytics at scale
- Reduce duplication and inefficiency
- Support evidence-based performance management
- Drive sustainable productivity gains

Without it, reform risks reinforcing fragmentation, increasing duplication, limiting productivity and undermining national consistency.

Moreover, interoperability must extend beyond policing. Policing operates within a wider Criminal Justice System that includes prosecutors, courts, probation, prisons and safeguarding partners. If data cannot move efficiently across these boundaries, the benefits of digital transformation within policing alone will be constrained. True public value will only be realised through cross-system interoperability.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Despite strong strategic appetite, the practical delivery of interoperability has proven challenging. Legacy architectures, varied procurement approaches and inconsistent adoption of standards have created complexity across the landscape.

This handbook is designed to move us from aspiration to implementation.

It brings together commonly agreed principles, standards and best practices that can be adopted now by digital, data and technology leaders across policing. It aligns with national strategy, reflects sector consensus and provides practical guidance to support consistent, standards-based delivery.

The decisions we make in procurement, design, governance and investment will determine whether policing evolves into a coherent, data-enabled national system or remains digitally fragmented.

By embedding interoperability into our strategies, architectures and delivery models, we can enable reform, unlock innovation and strengthen the effectiveness of policing and the wider criminal justice system.

Audience

This document will be helpful to local policing, national law enforcement agencies, policing partners and private sector organisations who provide or procure policing systems. It is also aimed at anyone within policing who is responsible for making data architecture or technical decisions for systems. This includes:

- Chief Information Officers
- Chief Data Officers
- Chief Technology Officers
- Chief Architects and Enterprise Architects
- Chief Digital Innovation Officers
- Programme managers
- Procurement
- Technology Directors

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Scope

The scope of this document is to simplify the process of making policing systems interoperable by explaining what interoperability is and how it can be implemented within a policing context. More specifically this includes the following:

- Provide policing with a clear definition of what interoperability is.
- Outline the policing benefits of making systems interoperable.
- Promote the adoption of common data models and standards.
- Explain what resources are available to help implement interoperable systems and where to find them.
- Promote the usage of a common vocabulary/terminology for describing policing systems and data.
- Establish and promote an API catalogue
- Incorporate interoperability and API requirements into policing procurement processes.
- Promote national and regional shared repositories.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Why Interoperability matters

Interoperable IT systems within policing form a crucial web of seamless communication and data exchange. By enabling different law enforcement agencies to effortlessly share information and collaborate, these systems enhance the ability to detect, prevent and respond to threats. Timely sharing of intelligence, suspect data and incident reports facilitates a comprehensive overview of criminal activities. This empowers law enforcement agencies to identify patterns, coordinate efforts, and deploy resources effectively. Ultimately, interoperability fosters a more cohesive response, ensuring that potential risks are addressed promptly and public safety is upheld with increased accuracy and efficiency.

Some of the challenges interoperable systems can help tackle are shown in the graphic on the next page.

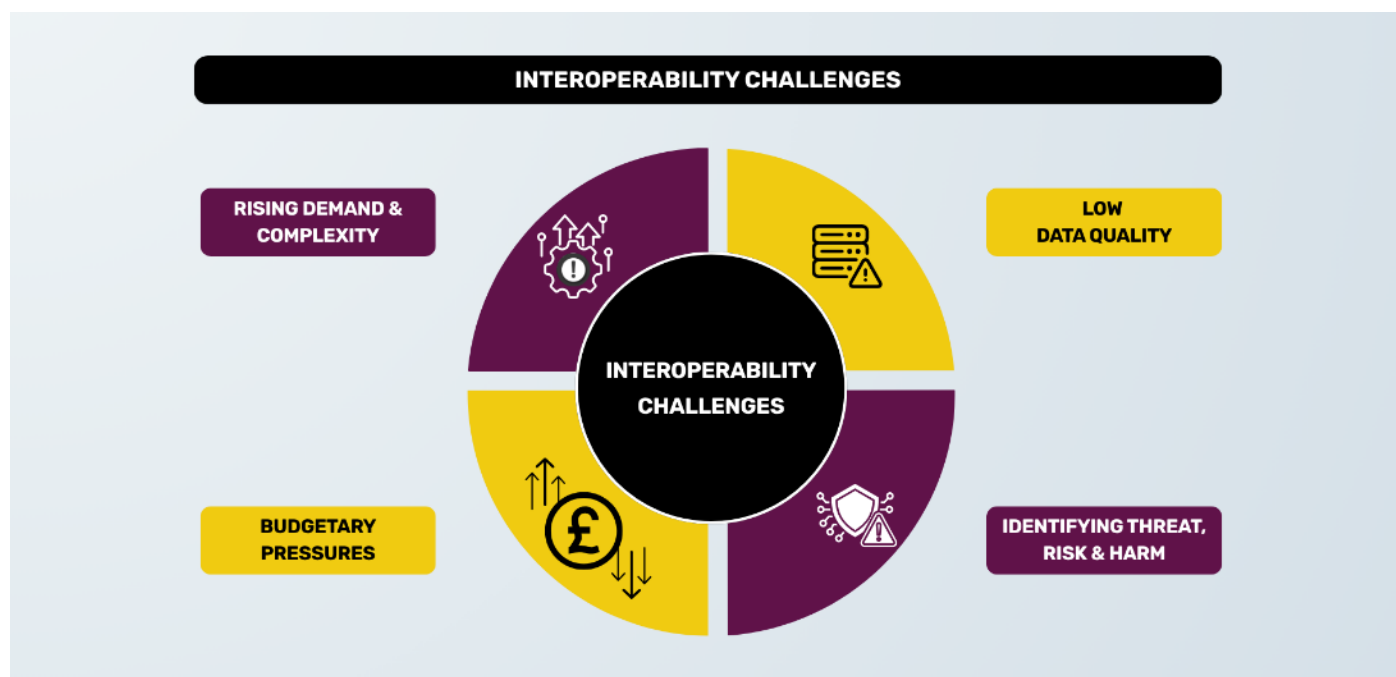


Figure 2 - Graphic showing challenges interoperable systems can help solve

Identifying threat, risk and harm. A greater number of data sets offers the possibility of greater insights, but only if those insights can be identified and interpreted, in an ever-increasing volume of data. In 2017 there were 220 different databases operated by individual police forces, often holding information in incompatible ways.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Budgetary pressures. Home Office statistics show that overall agreed police funding is projected to reach up to £19.6 billion by 2025/26¹. This represents a real-terms increase of up to 19.8% compared with 2015/16 levels. Despite this growth, police forces continue to face significant financial pressures linked to inflation, workforce costs, legacy technology, and increasing operational demand. Interoperable systems can therefore play a critical role in maximising efficiency by reducing duplication, streamlining processes, and enabling better use of available resources.

Rising demand and complexity. Police recorded crime showed an 8% increase as of the year ending September 2018. Increasingly complex cases demand greater resourcing. Converging on common data models and architecture patterns can reduce complexity and alleviate this pressure.

Low data quality. The combination of “system complexity” and large number of systems/solutions used within policing has resulted in a divergent data landscape. Measures are needed to establish a common data vocabulary that policing can converge on.

¹ Police Funding Settlement for England and Wales 25/26

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

What is interoperability?

This section will:

- Define interoperability.
- Outline the policing benefits of interoperable systems.
- Give an overview of what an interoperable system looks like.

There are several definitions of interoperability that vary slightly from industry to industry. The IEEE definition is the “**ability of a system or a product to work together with other systems or products without special effort on the part of the customer. Interoperability is made possible by the implementation of standards.**”² Whereas the NHSx³ defines it as “**the ability of two or more systems to share, communicate and cooperate.**”⁴

Summarising interoperability within a single sentence presents a challenge due to the inherent complexity of its four distinct layers. Before providing a definition, it is crucial to elaborate on these layers. This expanded definition is important as these layers serve as a benchmark against which we can measure success.

1. **Foundational Interoperability (Share).** At the basic level, systems can exchange data without requiring interpretation. This involves establishing a common mechanism for data transmission, often achieved through standardised communication protocols. However, the meaning and context of the exchanged data may not be fully understood or utilised.
2. **Structural Interoperability (Structured).** This level involves defining the structure and format of exchanged data, ensuring that both the sending and receiving systems understand the data’s syntax. Common data models, message formats, APIs and standards are used to facilitate accurate data exchange. NB. Structural interoperability is also referred to as syntactic interoperability, e.g. XML, JSON, CSV, HTTP, SOAP.
3. **Semantic Interoperability (Meaningful information).** Here, systems not only exchange data in a structured format but also understand the meaning and context behind the data. This requires metadata, shared ontologies, vocabularies, and data dictionaries to ensure that data is interpreted correctly and consistently across different systems.

² [Standards Glossary | IEEE Standards University](#)

³ [NHSX: new joint organisation for digital, data and technology - GOV.UK \(www.gov.uk\)](#)

⁴ [Interoperability Handbook v1.0 \(england.nhs.uk\)](#)

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

4. **Organisational Interoperability (Across organisational boundaries).** The highest level of interoperability involves alignment between entire organisations or ecosystems. This goes beyond technical aspects and involves harmonising business processes, policies and procedures. It requires collaboration, governance and a shared commitment to achieving common goals.

Interoperability Definition

In a policing context, the official PDS definition of interoperability is:

The ability to share structured, meaningful information across organisational boundaries.

This sector-wide endorsed definition reinforces alignment with both the National Policing Digital Strategy 2025–2030 and the National Policing IT Reform Strategy and Roadmap. It will serve as a benchmark for measuring progress and enable us to concisely describe interoperability in a manner understandable to stakeholders. The following diagram highlights the levels of interoperability along with some examples.

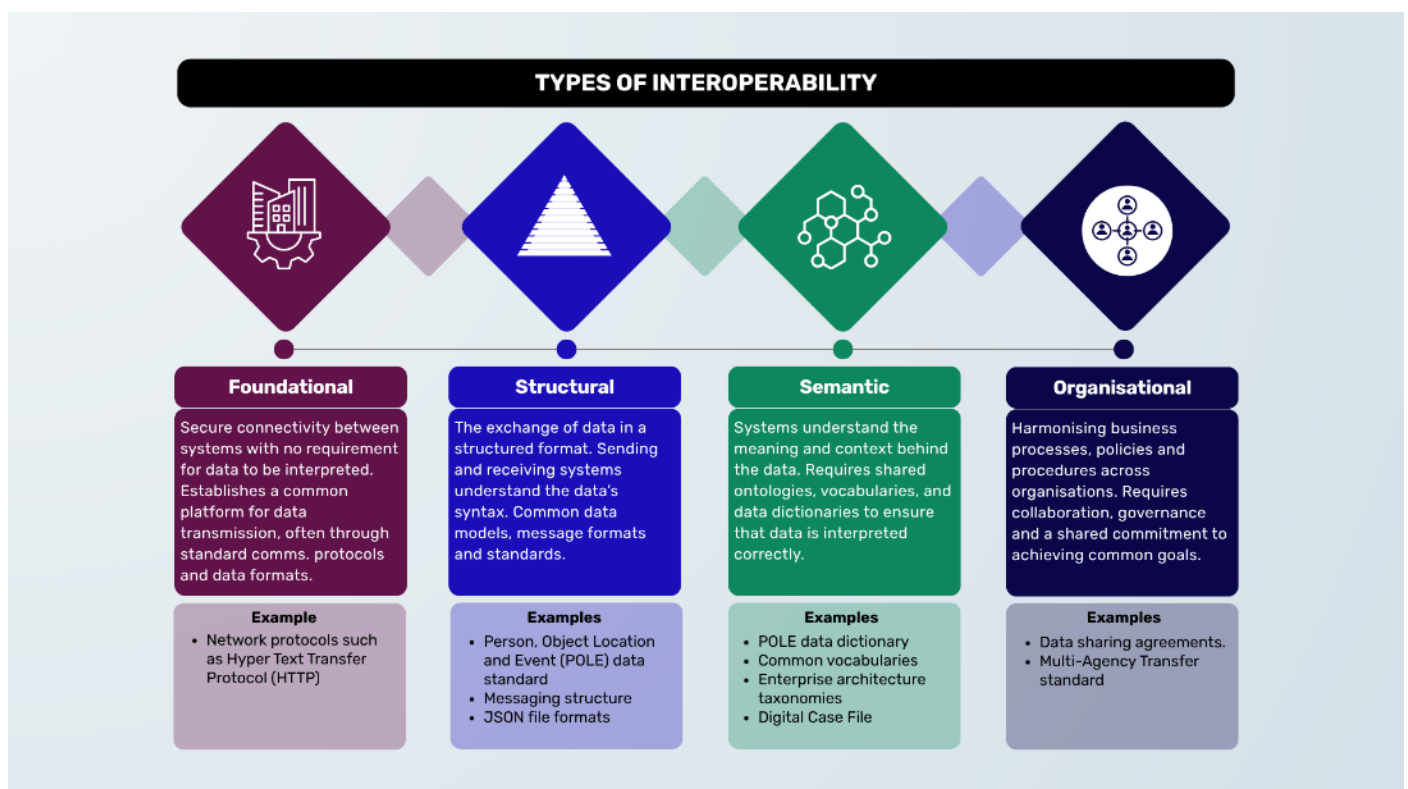


Figure 1 – Graphic showing types of interoperability with examples

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Interoperability in policing. Example

Illustrating these various levels of interoperability in a policing scenario, consider the following example:

A crime is reported online via the Single Online Home (SOH) system. The user's device securely connects to the SOH using internet protocols, demonstrating foundational interoperability. The user provides a detailed crime report, transmitted to the SOH using a JSON formatted message file, highlighting structural interoperability. At this point, data has been securely exchanged but its significance and appropriate actions remain undefined.

Subsequently, the SOH processes the data utilising a shared data model and dictionary like POLE and discerns that the reported crime falls under the jurisdiction of a specific police force, thus accomplishing semantic interoperability. The information is then communicated to the force through an established data sharing agreement, demonstrating organisational interoperability.

What Does an Interoperable System look like?

An interoperable ecosystem will be able share meaningful information efficiently with no need for manual activities (such as double keying the same information into two different systems). The information displayed is accurate and formatted correctly with no need for any manipulation. The information will be available to whoever needs it when they need. A robust governance structure is in place to swiftly address any discrepancies.

Interoperable systems typically have the following characteristics (see graphic below).

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

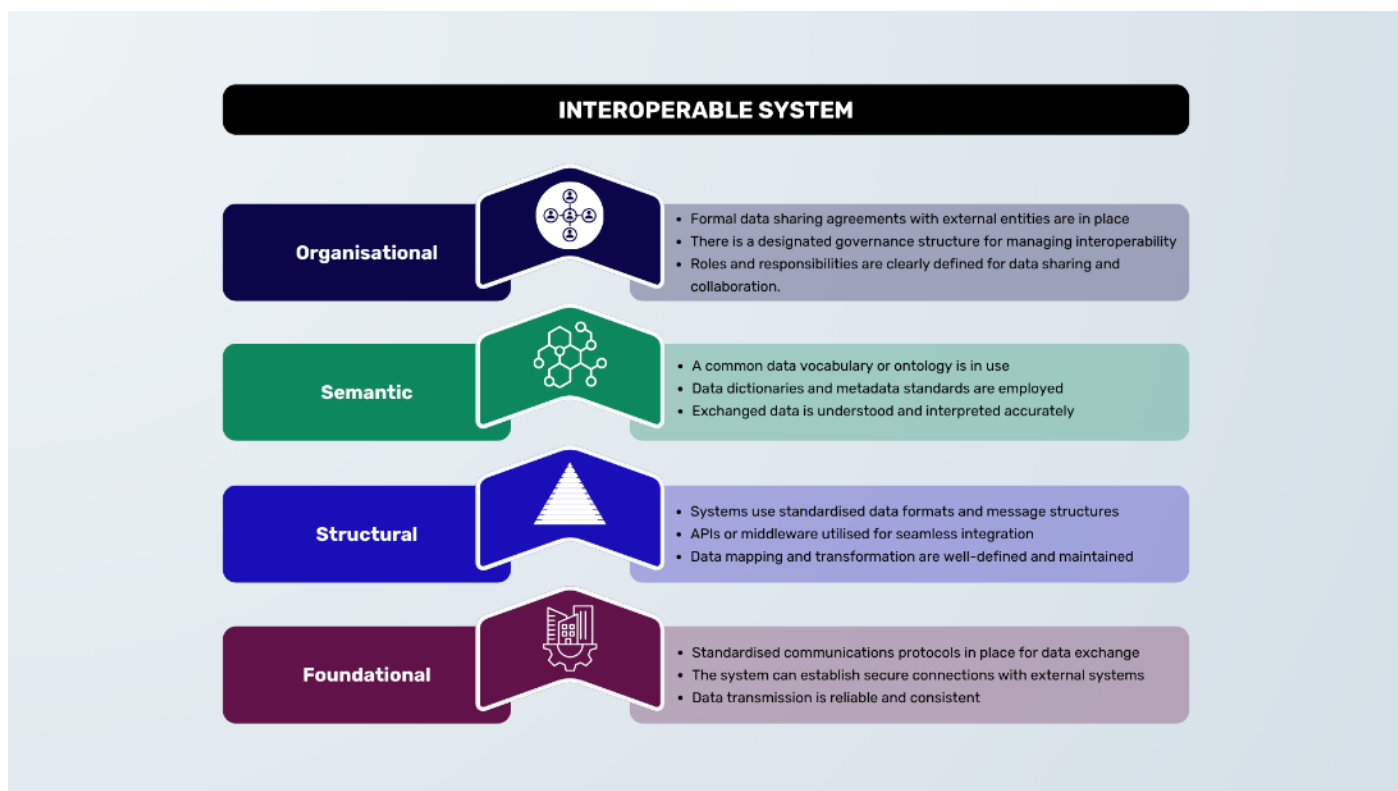


Figure 3 - Characteristics of interoperable systems

DATE:	17 July 2026
VERSION:	1.0
DOCUMENT REFERENCE:	

COPYRIGHT:	
NUMBER OF PAGES:	38
CLASSIFICATION:	OFFICIAL

Interoperability Maturity Assessment

Assessing your maturity level will reveal strengths, weaknesses and help you create a clear improvement path. This evaluation will enhance decision-making and is a significant part of your interoperability journey.

This section will provide a set of actions to perform to help assess your organisations level of interoperability maturity. This assessment is for guidance only and you should also consider the specific connectivity, data and security requirements of your systems.

The maturity and benefits of interoperability increase with each level of interoperability that you achieve. It should be noted that foundational and structural interoperability are normally pre-requisites for semantic interoperability; systems must structure data in a common way before it can be interpreted and understood using a common vocabulary.

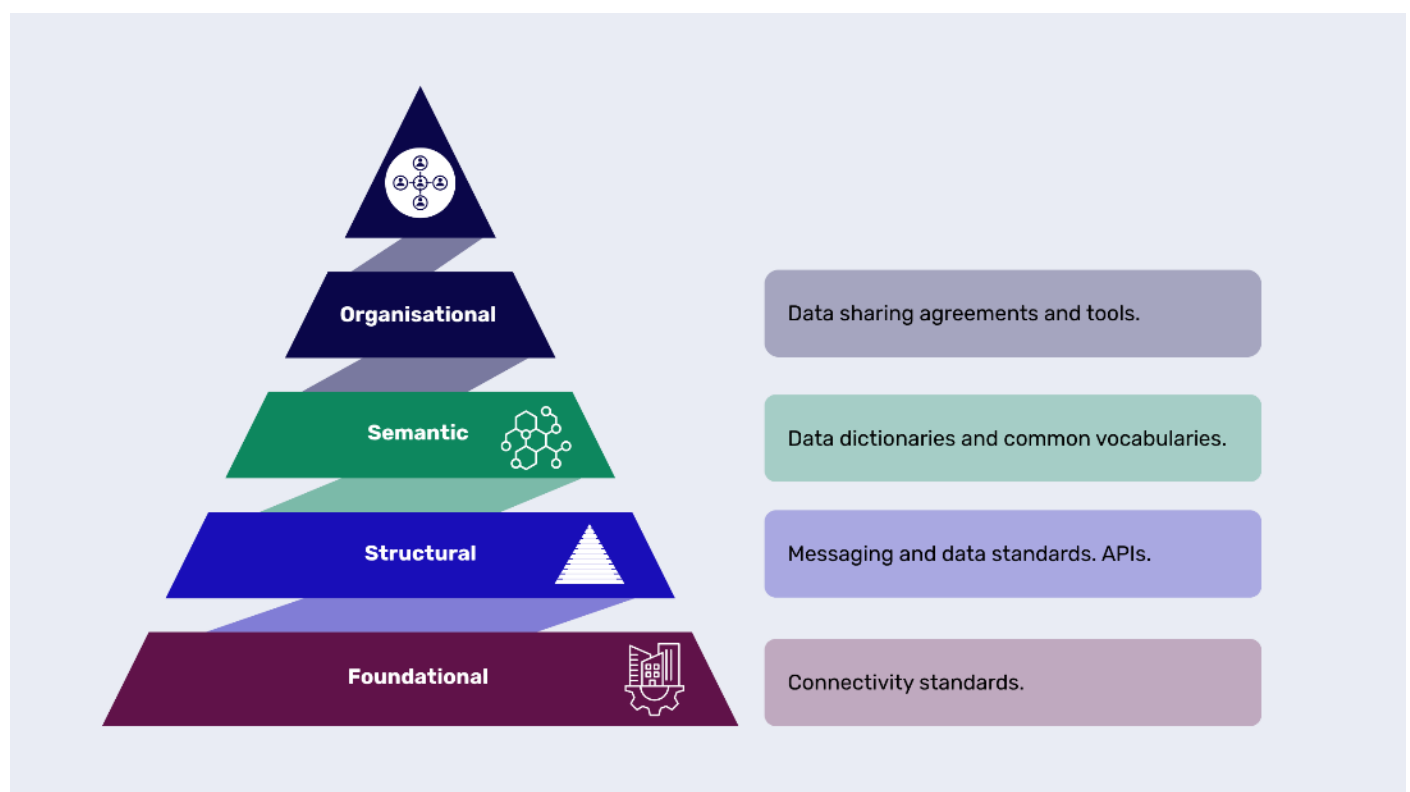


Figure 5 - Graphic showing inceasing maturity and benefits progressing through interoperability layers

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

FOUNDATIONAL INTEROPERABILITY ASSESSMENT

The assessment is intended to identify areas for improvement. It contains a set of activities and questions that can be applied to a system to determine which level(s) of interoperability needs to be focused on. You can then refer to the description of that level to determine what resources you can use to assist you on your interoperability journey.

FOUNDATIONAL INTEROPERABILITY ASSESSMENT	
Review Connectivity Standards	Check if the system adheres to widely accepted connectivity standards, such as TCP/IP for internet communication. These standards ensure that the system can establish basic connections with other systems.
Assess Network Connectivity	Assess whether the system can seamlessly connect over common network infrastructures including LANs, WANs, the internet and, the PSN.
Examine Network Protocols	Verify whether the system uses standardised network protocols for basic communication, such as HTTP or IP addressing and routing protocols, which are essential for data transmission.
Test Basic Connectivity	Conduct basic connectivity tests to confirm that the system can establish connections with other systems or devices. This can include ping tests or simple network communication.
Check for Firewall and Security Compatibility	Ensure that the system's security features, including firewalls and authentication mechanisms, are compatible with commonly used security standards.
Evaluate Data Transmission	Assess the system's ability to transmit data reliably and securely over networks, including error handling and data integrity checks.
Examine Network Scalability	Determine if the system can scale to accommodate increased network traffic and data volume, ensuring it remains functional as your needs grow.
Review Network Infrastructure Documentation	Examine the system's documentation to understand how it interacts with network infrastructure components like routers, switches, and gateways.
Conduct Basic Network Tests	Execute network connectivity tests, including checking for open ports and the ability to connect to external systems. Successful network interactions indicate foundational interoperability.

By following these steps, you can assess whether a system possesses the foundational

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL



interoperability required to establish basic network connections and communicate with other systems effectively.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

STRUCTURAL INTEROPERABILITY ASSESSMENT

Assessing your structural interoperability maturity level involves evaluating how well your organisations data and systems adhere to standardised formats and structures for seamless data exchange.

STRUCTURAL INTEROPERABILITY ASSESSMENT ELEMENTS	
Examine Data Exchange Standards	Are universally accepted data exchange standards used for communication (such as JSON or XML)? Consistent data formats promote smooth data exchange and integration.
Check for API Availability	Assess whether the system provides Application Programming Interfaces (APIs) that enable other systems to interact with it. APIs facilitate structured data exchange.
Evaluate Message Structure	Determine if a system follows a predefined message structure or schema when exchanging data. This ensures that data is organised and understandable by other systems.
Assess Integration Tools	Investigate if the system offers integration tools or middleware that simplify the process of connecting with other systems.
Test Data Mapping and Transformation	Verify if the system can map and transform data from one format to another, ensuring compatibility between different systems.
Analyse Error Handling	Examine how the system handles errors during data exchange. Robust error handling mechanisms indicate a well-structured system.
Verify Metadata Usage	Look for usage of metadata or annotation that provide additional context and information about the exchanged data.
Review Documentation	Study the systems documentation to understand how it interacts with other systems and whether it adheres to structural interoperability practices.
Conduct Integration Testing	Perform integration testing by attempting to exchange data with other systems. Successful data exchange without significant challenges indicates structural interoperability.

By following these steps, you can assess whether a system is structurally interoperable and capable of effectively exchanging data with other systems while maintaining consistency and integrity.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

SEMANTIC INTEROPERABILITY ASSESSMENT

Assessing your semantic interoperability maturity level involves your ability to exchange and understand information consistently and meaningfully across different systems.

SEMANTIC INTEROPERABILITY ASSESSMENT ELEMENTS	
Common Data Models	Ensure that the system(s) share common data models that define the meaning of the data (not just the structure), allowing for consistent interpretation across systems.
Terminology and Vocabulary	Assess whether the system employs standardised terminology, ontologies, or controlled vocabularies. These ensure consistent interpretation of data elements.
Metadata Usage	Verify if the system includes metadata with data exchanges. Metadata provides additional context about the data, aiding in understanding and interpretation.
Semantic Mapping	Analyse how the system maps and transforms data between different formats while preserving meaning and context. This is crucial when integrating with systems using varied data models.
Common Reference Data Sets	Are common reference data sets used? For example, UK postcodes, ISO country codes or third-party data sets (e.g. DVLA). Common reference data sets allow effective information
Semantic Validation	Check if the system validates incoming data for semantic accuracy. It should ensure that data adheres to expected meanings and business rules.
Semantic Annotations	Look for semantic annotations within data or messages that provide explicit information about the intended meaning of data elements.
Ontology Compatibility	Ensure that the system's data representation aligns with policing-specific or domain-specific ontologies, enhancing shared understanding.
Interpretation and Inference	Assess whether the system can infer additional information or context from received data, enabling more comprehensive understanding.
Documentation and Compliance	Review documentation to determine if the system complies with established semantic standards and practices relevant to policing.
Testing with Real Data	Perform tests using real-world data to validate that the system correctly interprets and uses data according to the intended meaning.

DATE:	17 July 2026
VERSION:	1.0
DOCUMENT REFERENCE:	

COPYRIGHT:	
NUMBER OF PAGES:	38
CLASSIFICATION:	OFFICIAL

ORGANISATIONAL INTEROPERABILITY ASSESSMENT

Assessing the maturity level of organisational interoperability involves evaluating how well your organisation can collaborate, share data, and work seamlessly with other entities. Here are tasks that will help you assess your organisational interoperability maturity level.

ORGANISATIONAL INTEROPERABILITY ASSESSMENT ELEMENTS	
Review Data Sharing Agreements	Check if the systems have formal data sharing agreements or Memoranda of Understanding (MoU) in place with other organisations or agencies. These agreements should outline the terms, conditions, and protocols for sharing data and collaborating.
Evaluate Governance Structure	Assess whether there is a clearly defined governance structure for managing interoperability efforts. This structure should include roles, responsibilities, and decision-making processes related to data sharing and collaboration.
Interagency Coordination	Investigate the extent to which the system coordinates and collaborates with other agencies and organisations. This includes regular meetings, communication channels and shared objectives.
Data Access Control	Verify how the system controls access to shared data. It should have mechanisms in place to grant or restrict access based on agreed upon permissions and security protocols.
Compliance with Regulations	Ensure that the system complies with relevant data privacy and security regulations, especially when sharing data across organisational boundaries.
Data Ownership and Stewardship	Clarify data ownership and stewardship responsibilities. This includes identifying who is responsible for data maintenance, updates, and quality assurance.
Documentation and Reporting	Review the documentation related to data sharing agreements, governance, and compliance. Ensure there is a process for reporting on the progress and status of interoperability initiatives.
Test with Partner Organisations	Conduct tests and simulations with partner organisations to verify the effectiveness of data sharing and collaboration processes.
Conflict Resolution Mechanisms	Identify the mechanisms in place for resolving disputes or conflicts related to data sharing and collaboration.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Planning for Interoperability

Enhancing interoperability within policing needs a systematic approach that aligns objectives, evaluates existing conditions, addresses gaps, accounts for resource allocation and outlines a well-structured plan. The graphic below gives an overview of how you can start your interoperability journey. The pages that follow break this down to provide additional guidance for each phase in the journey.

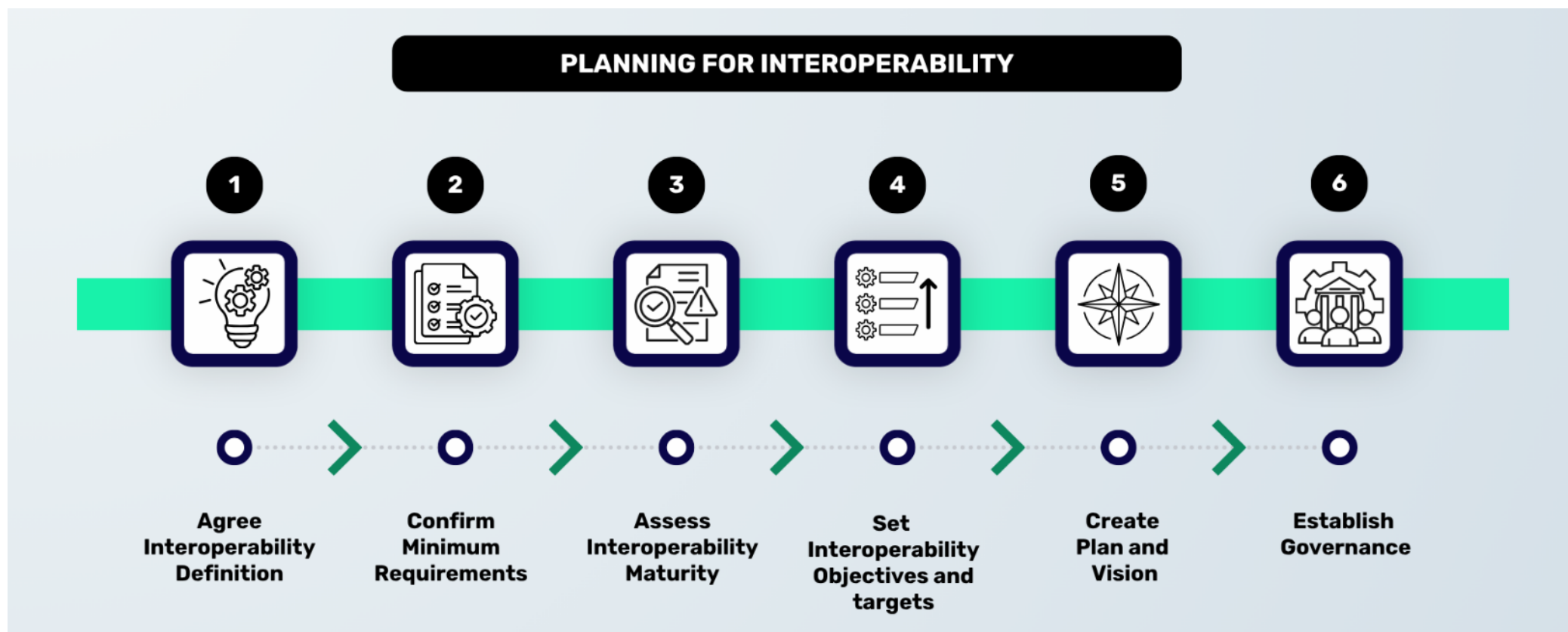


Figure 6 - Graphic giving an overview of an interoperability journey

1. Agree on a common definition of interoperability for policing:

Agreeing on a common definition of interoperability is key for ensuring consistency in planning and tracking the progress of interoperability initiatives. Your interoperability journey may span years and involve numerous workstreams and stakeholders, establishing a policing wide definition before beginning any work is crucial.

Key considerations at this stage:

- 1.1. Define interoperability
- 1.2. Review definition
- 1.3. Publish definition
- 1.4. Interoperability Handbook (reference point).

2. Define the minimum acceptable interoperability requirements:

A range of resources including communication protocols, standards, guidance and best practices are available to help you implement each layer of interoperability. Objectively determining which ones are the minimum requirements will help you develop a realistic plan. Key considerations at this stage:

- 2.1. Minimum Foundational requirements
- 2.2. Minimum Structural requirements
- 2.3. Minimum Semantic requirements
- 2.4. Minimum Organisational requirements
- 2.5. Minimum supporting requirements

3. Assess your current level of interoperability maturity and document the gaps:

Assess your current level of interoperability. Evaluate your systems explicitly looking at the following:

- Data standards
- Messaging and data exchange formats
- Data models/dictionaries
- Communication protocols
- adherence to existing standards
- Data sharing agreements

What is the level of compliance with interoperability standards that are hosted on the [National Standards Platform](#). This assessment will help you identify your strengths and weaknesses. You should also use interoperability assessments to benchmark your current status. Compare this against your target level. Document discrepancies in foundational, structural and semantic interoperability. Highlight areas where you are not meeting standards and guidance. Staying with the example of DII, you can assess your systems against the [Digital Asset Management Standards \(DAMS\)](#) maintained by the College of Policing; this standard specifies the requirements for structural and semantic interoperability.

Key considerations at this stage:

- 3.1. Assess maturity levels

3.2. Document the gap from minimum requirements

4. Establish your objectives/targets:

With a clearer definition of what interoperability is we can define clearer goals. Are you aiming to streamline information sharing between law enforcement agencies or improve data accuracy? Set specific, measurable, achievable, relevant and time-bound (SMART) objectives. The graphic below provides some example objectives.

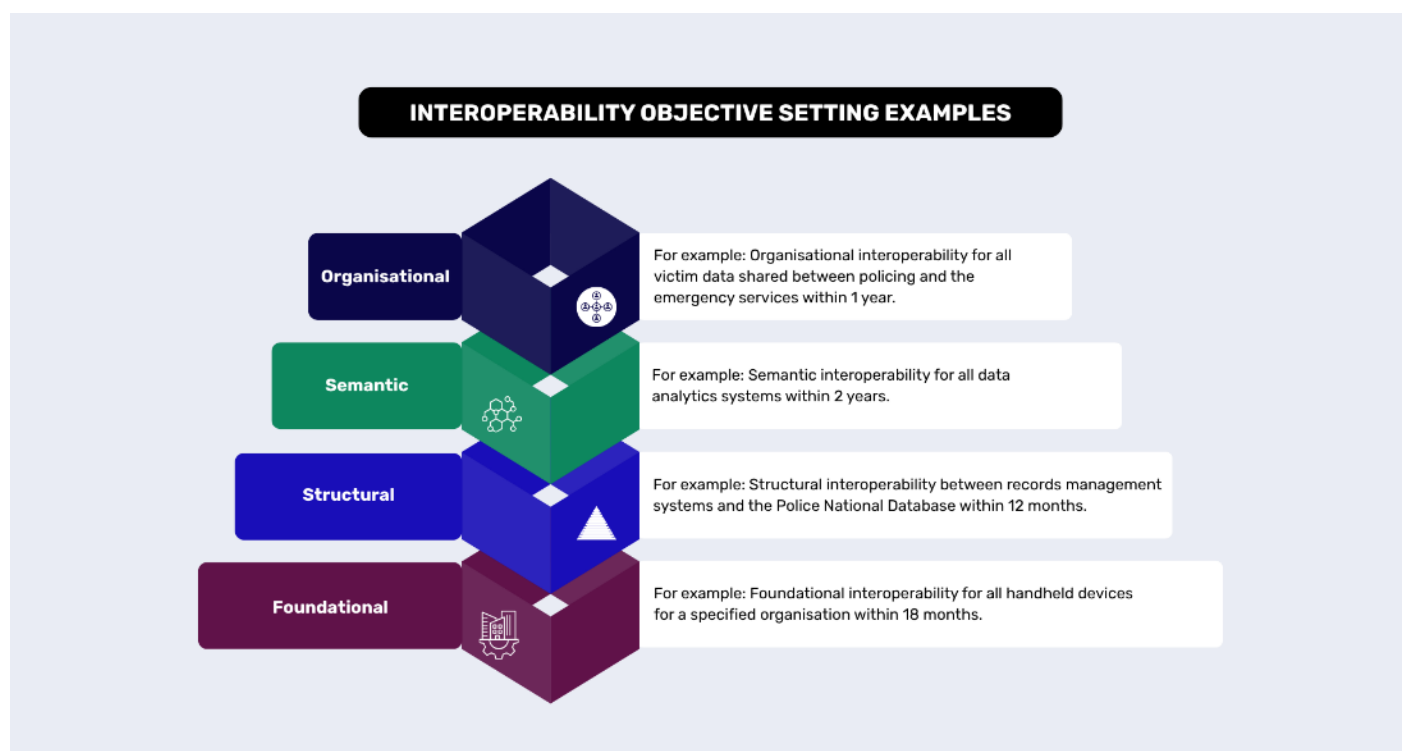


Figure 7 - Graphic showing examples of objectives that can be set for each interoperability layer

You might aim to achieve foundational interoperability for devices within a particular force within 18 months, or semantic interoperability within the digital intelligence & investigation (DII) ecosystem within two years. A common and detailed definition of interoperability allows us to set specific targets and create more realistic plans. Key considerations at this stage:

- 4.1. Define minimum objectives
- 4.2. Define additional objectives

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

5. Create your vision and plan and align it with the National Policing Digital Strategy:

Develop a detailed plan that addresses identified gaps. Outline specific actions, milestones, timelines, and responsible stakeholders. Consider factors like technology upgrades, staff training, and process adjustments. Assign accountability to ensure progress tracking. Key considerations at this stage include:

- 5.1. **Short-Term Solutions.** Address immediate gaps with quick fixes, such as data format conversions.
- 5.2. **Mid-Term Strategies.** Implement measures like adopting shared data models and refining communication protocols.
- 5.3. **Long-Term Vision.** Work toward semantic and organisational interoperability through collaborative efforts and comprehensive data strategies.

Acknowledge competing priorities that might vie for resources. Balancing interoperability improvements with other pressing needs is crucial. Understand resource constraints and identify potential synergies with ongoing projects. For example, can data and messaging standards be included in the requirements of other new projects? Increasing your level of interoperability is no small task and may require strategic planning and collaboration across several law enforcement agencies.

6. Establish governance:

Use existing national policing boards to resolve interoperability issues. National policing boards can provide governance and direction that aligns with existing policing. By following this approach, law enforcement agencies can incrementally bridge the interoperability gaps, align with standards, and enhance overall efficiency and effectiveness in their operations. Regularly monitor progress and adjust the plan as necessary to achieve the desired level of interoperability. Key considerations at this stage include:

- 6.1. Standards governance
- 6.2. Data governance
- 6.3. Technical governance
- 6.4. Supplier engagement

Interoperability and Suppliers

Selecting a supplier whose systems prioritise interoperability holds immense strategic value. Interoperable systems connect and communicate with existing infrastructure, fostering operational efficiency and adaptability. This compatibility streamlines data exchange, preventing silos and enhancing collaboration across departments and functions.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

An interoperable supplier empowers organisations to integrate new technologies without disrupting established processes. This flexibility aids future scalability and innovation, positioning the organisation at the forefront of advancements.

Moreover, interoperable systems reduce dependence on a single vendor, mitigating risks associated with vendor lock-in. This safeguards against potential constraints on system expansion, upgrades, or modifications.

In the rapidly evolving landscape of IT, interoperability is the cornerstone of agility. A supplier committed to this principle demonstrates their commitment to long-term partnership, enabling organisations to optimise resource allocation, stay current with industry trends, and efficiently adapt to dynamic challenges.

Assessing a supplier's level of interoperability

We now have the knowledge to articulate interoperability to suppliers, this section will provide guidance on how to engage with suppliers and discuss the level of interoperability of their system/ecosystem.

You should understand how interoperable vendor solutions are:

- Are their APIs open, standard or propriety? How are the APIs licensed? Read the Application Programming Interfaces section of this document for more information.
- Does the solution adhere to any of the interoperability standards on the [National Standards Platform](#)?
- Do they use open source standards?
- How does the system handle non-textual information such as videos and images? Do they need to be manipulated in a way that would invalidate their authenticity before they are transmitted to another system?
- Does the solution use any information exchange standards such as JSON or XML? Do these exchange formats align with the other systems it will integrate with?
- Does it use a compatible data standard such as POLE? Is any data manipulation or formatting required before it can be viewed correctly in the viewing system?
- Can the system transmit securely and reliably using the preferred policing network protocols? Does it adhere to cybersecurity connectivity standards?
- Review the product roadmap in detail. Does the supplier plan to maintain the system to keep it compatible with policing platforms?
- Are their products compatible with national policing platforms such as the National Management Centre (NMC)?

The techUK interoperability in Justice and Public Safety forum works to improve the interoperability systems provided by the private sector. Suppliers are encouraged to sign up to techUK's interoperability charter.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Interoperability Resources

This section will explain how to access important interoperable resources that you can start using now. All the standards and tools listed here have been reviewed and approved either by a policing organisation or an appropriate subject matter expert group from industry.

Resources are grouped by their interoperability layer, and they will cover the following:

- Data/document repositories
- Connectivity standards
- Data standards and data models
- APIs
- Inter-agency data sharing agreements

Foundational Interoperability Resources

Connectivity Standards

Connectivity standards are established guidelines and protocols that define how different systems, devices or components should communicate or interact with each other. These standards ensures compatibility and data exchange between disparate technologies regardless of their origins or purpose. Some notable examples include HTTP protocol, TCP/IP and Wi-Fi.

- [National Standards Platform](#). As well as improving interoperability, National Standards for data and technology in policing can help to drive innovation and reduce costs. The development of National Standards brings together UK policing, the Home Office and suppliers, in a common approach to sourcing, promoting and adopting standards in line with the National Policing Digital Strategy. You will find a range of standards including connectivity standards on the platform.
- [Frontline Digital Mobility - Connection Types](#). This guidance will explore the main connection types used by frontline officers and staff, whilst making recommendations about security and appropriate use. This guideline focuses on assisting forces to maximise their use of public data networks prior to the delivery and adoption of the Emergency Service Network Data Services. This guideline does not cover voice services delivered over any of these networks.
- [Frontline Digital Mobility - Portable Hotspots](#). Portable hotspots are a tried and tested peripheral. Advances continue to make them faster, better and smaller. There are many types of portable hotspots available in the marketplace with many variances in terms of specification, features and of course price. This guideline explores these variances and makes recommendations (see section 4. Recommendations, page 3) to help forces make informed selections to accelerate their mobility maturity.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

- [Wi-Fi \(IEEE802.11\)](#). These standards govern wireless local area network (LAN) communication, allowing devices to connect to the internet and each other wirelessly. Common variations include 802.11n and 802.11ax (Wi-Fi 6).
- [Ethernet \(IEEE 802.3\)](#). Ethernet standards govern wired LAN communication, with variants like 1000BASE-T and 10GBASE-T specifying data rates and cable types.
- [HTTP \(Hypertext Transfer Protocol\)](#). HTTP and its secure variant, HTTPS, are standards for data exchange on the world wide web, facilitating communication between web servers and browsers.
- [NIST](#) and [NCSC](#) approved connectivity protocols and guidance.

Structural Interoperability Resources

Data Standards

Data standards are established guidelines and specifications that define how data should be formatted, structured, and represented. They provide a common framework for organising and presenting information, ensuring consistency and interoperability across different systems, applications, and organisations. Data standards encompass various aspects, including data formats, naming conventions, data types, units of measurement and more.

- [POLE Data Standards Catalogue](#). The intended purpose of this standard is to promote interoperability and improve the data quality of systems by converging on a common set of POLE data definitions used within Policing. POLE data definitions describe how People, Objects, Locations and Events (POLE) should be formatted.
- [Police National Database \(PND\) Interface Business and Technical Guidance for Data Providers](#). This document provides an overview of data requirements including message schema design and data transmission mechanisms.
- [Open Referral UK Standards](#). Open Referral UK is an open data standard in use by Local Government. This standard establishes a consistent way of publishing and describing information for councils, to ensure the data is effectively used and shared for the benefit of local communities and services.
- [Data Protection Manual](#). The Data Protection Manual provides guidance on the rules and governance that are in place to enforce GDPR within policing.

Messaging Formats

Message format standards facilitate data exchange, integration, and interoperability among diverse systems and applications, making it possible for organisations to communicate effectively and share data in a standardised way. The following points provide links to useful reference material.

- [JSON](#) is a lightweight, text based data interchange format that is designed to be easy for both humans to read and write and also machines to parse and generate.
- [XML](#) is similar to JSON in that it is also designed to be readable by humans and easy for machines to parse.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

- [YAML](#) is a human readable data serialisation format that is often used for configuration files and data exchange between programs. Unlike XML and JSON, which use explicit markup or delimiters, YAML relies on indentation and whitespace to represent data hierarchies and structure.

Application Programming Interface (API)

An API, or Application Programming Interface, serves as a bridge between software applications, enabling them to communicate and interact seamlessly, sharing data and functionalities.

Using APIs yields multifaceted advantages. They expedite development by reusing existing code, enhance collaboration, enable third party integrations, boost innovation through modular design and simplify complex processes, driving efficiency and flexibility. If they are used in a consistent fashion APIs are an excellent way of improving the interoperability of policing systems, as shown in the graphic below.

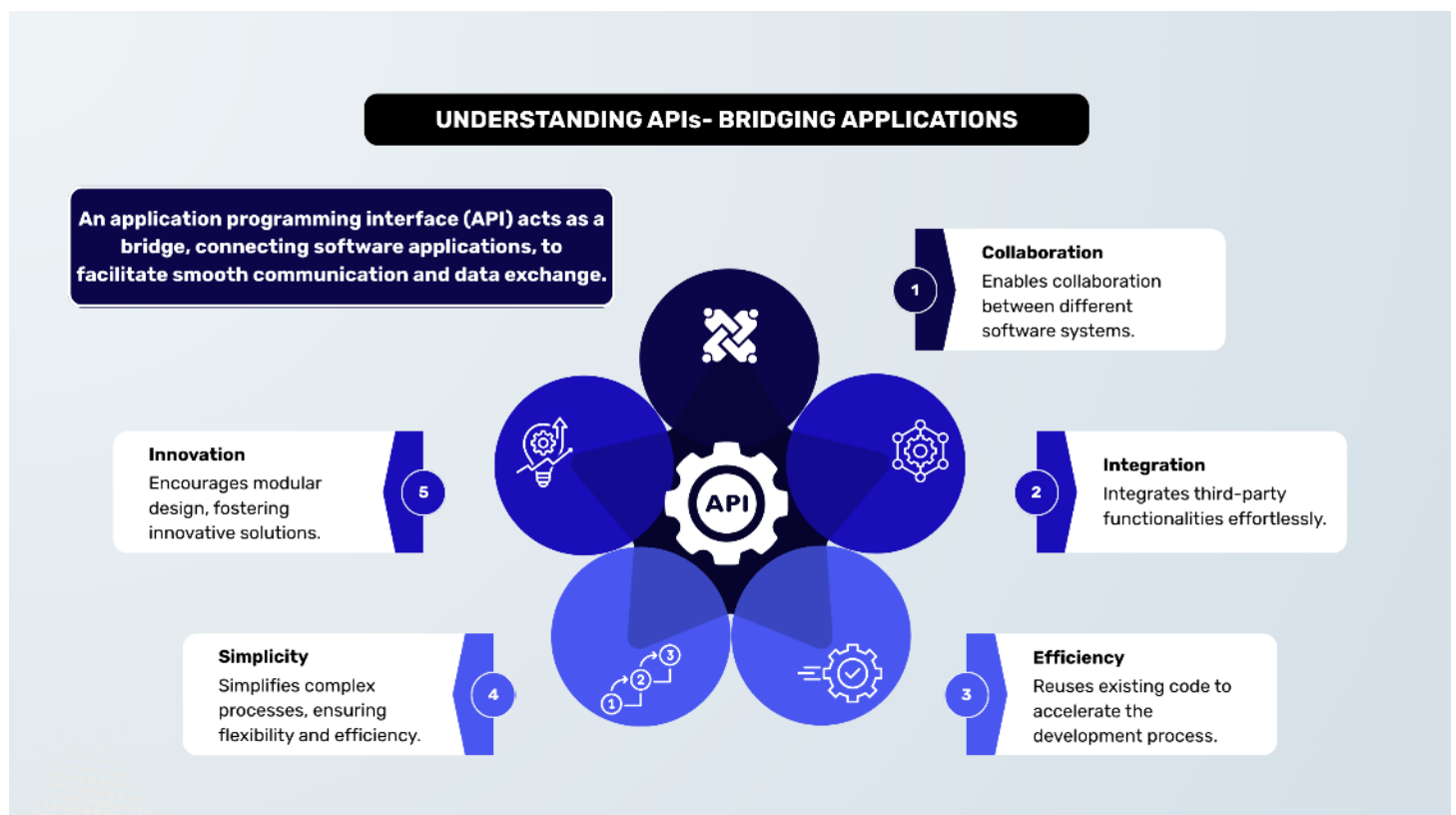


Figure 8 – Graphic showing the benefits of APIs for supporting interoperability.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

There is guidance available on how to create and maintain APIs (listed below). This guidance is supported by the National Standards Assurance Board and the National Technical Design Authority and should be followed wherever possible to promote interoperability.

- **Creating and maintain APIs.** The OpenAPI Specification (OAS) is a standard for describing your APIs. More information on creating an OAS can be found [here](#) from the OpenAPI Initiative where you will also be able to access the specification. You should use JSON as your specification language.
- **API Catalogue.** A catalogue of existing APIs has been created and can be accessed from the [National Standards Platform](#). This catalogue contains APIs for many policing systems.

It is important to note the differences between open, standard and propriety APIs, especially when assessing a third-party's use of APIs. Each will differ in terms of their accessibility, ownership and, most importantly their adherence to industry standards.

Open APIs

- **Accessibility:** Open APIs are publicly available for use by developers, typically without restrictions or fees. They are accessible to a wide range of users and developers.
- **Ownership:** Open APIs are often maintained and governed by open standards organisations or industry consortiums. They are not controlled by a single entity, and decisions regarding changes or updates are made collectively.
- **Standards:** Open APIs may adhere to open standards, ensuring that they are widely compatible and can be implemented across different platforms and technologies.

Standard APIs

- **Accessibility:** Standard APIs refer to widely accepted and used APIs in a particular industry or domain. They are accessible to developers who work within that industry.
- **Ownership:** Standard APIs can be owned and maintained by industry standards organisations, but they can also be developed and managed by a specific company or consortium.
- **Standards:** Standard APIs are designed to follow industry best practices and are intended to be used consistently across the industry. They often have some level of consensus among stakeholders.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Proprietary APIs

- **Accessibility:** Proprietary APIs are owned and controlled by a single company or organisation. Access to these APIs may require permission or a licensing agreement. They are typically restricted to a specific group of developers or partners.
- **Ownership:** Proprietary APIs are entirely owned and managed by the organisation that created them. This means the organisation has full control over changes, updates, and usage policies.
- **Standards:** Proprietary APIs may or may not follow industry standards. They are designed primarily to serve the specific needs and goals of the organisation that owns them.

Semantic Interoperability Resources

Ontologies

An ontology is a formal, structured representation of knowledge within a specific domain or field of study (for example intelligence). It defines concepts, relationship, entities, and properties in a way that allows for a shared understanding and interpretation of information. Ontologies are used to organise and represent complex information, facilitating data integration, knowledge sharing, and reasoning in various applications. They provide a framework for both humans and computers to comprehend and work with complex domain-specific knowledge effectively. Here are some example ontologies:

- [Semantic web ontology](#). [RDF](#) (Resource Description Framework) and [OWL](#) (Web Ontology Language) are used to create ontologies for the semantic web, allowing machines to understand and reason about web data.
- [Information Exchange Standard 4](#). IES 4 was developed by the UK Government with contributions from Dstl, Ministry of Defence, Metropolitan Police Service, Foreign & Commonwealth Office, Home Office, Department for Business and Trade (was BEIS), and HMRC, with technical support from Aurora Consulting (to Home Office) and Telicent (to Dstl). The purpose of the IES is to make Information exchange easier by providing a common vocabulary for data / information exchanges between knowledge stores. Information from each store is converted to / from the common vocabulary when it travels. Users and systems no longer need to understand many different formats and schemas. Each system only has to understand the relation between its own internal model and that of the IES, dramatically reducing complexity. From v4.0.0, the IES is specified as an RDF Schema. RDF is a standard published by the World Wide Web Consortium (W3C) and is the preferred data exchange format in UK Government.
- [Digital Case File](#). The Digital Case File national programme has established how case files are built and sent to the Crown Prosecution Service through collaboration with suppliers and police forces. This is the national standard required for any digital case file solution.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Organisational Interoperability Resources

Document Sharing Repositories

A shared document repository is a centralised digital space where multiple users can store, access, and collaborate on various types of documents. It serves as a secure and organised hub for files, offering features like version control, access permissions and search functionalities. While these are primarily aimed at collaboration at a team level they also allow for the secure sharing of documents nationally within accessed controlled environment. Here are some examples of sharing information.

- [The Knowledge Hub](#). Created and managed by the Police Digital Service, the Knowledge Hub is a secure, mobile web-based platform that enables police forces and other public-sector organisations to establish groups and networks to share information, discuss ideas and work more collaboratively.
- Microsoft Teams. The National Enabling Programme (NEP) enabled policing to use data and file sharing capabilities.

Inter-Agency Data Sharing Agreements

There are a number of data sharing agreements and data sharing tools available to use now.

Multi Agency Incident Transfer standard (MAIT). The exchange of incident information between key organisations such as the Police Force, Highways England, Ambulance Service, Fire service is critical to saving lives and keeping members of the public safe. The exchange of key information between organisations using command and control systems that manage incidents and deployments are used through formatted messages using extensible markup Language (XML). The Multi Agency Incident Transfer standard can be found [here](#) on the [National Standards Platform](#); it describes the implementation guidelines for exchanging information between multiple command and control systems between different organisations (Multi Agency Incident Transfer (MAIT), describe communications and data management issues that need to be considered, whilst providing suitable implementation guidance as well as describing interfaces available and their XML.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Interoperability Strategy

The interoperability strategy will help decision makers explain the benefits of interoperability and guide them on their journey. It is also an enabler for policing and its purpose is to support the National Policing Digital Strategy deliver on its key objectives.

The National Policing Digital Strategy

1. **Seamless citizen experience.** We will deliver seamless, digitally enabled experiences. The public will have more choice in how they engage with police forces, using channels, media or devices most relevant to them. We will be able to connect citizen interactions, information and data across departments, and across forces to build a more credible and richer intelligence picture, all whilst maintaining public trust by ethically acquiring, exploiting and sharing their data.
2. **Protect the public.** We will harness the power of digital technologies and behaviours to identify the risk of harm and protect the vulnerable in the physical and digital world. We will deliver earlier, more precise and targeted proactive policing approaches and early interventions through the application of digital technology.
3. **Enable officers and staff through digital.** We will invest in our people, from leadership through to the front-line, to ensure they are equipped with the right capabilities (knowledge, skills and tools) to deal with increasingly complex crimes. We will establish digital leadership and ways of working to allow our workforce to focus on critical and value-adding activities.
4. **Embed a whole public service approach.** We will foster a philosophy of openness and deepen our collaboration with our public sector partners to jointly design and tackle complex public safety issues - sharing data insights and making use of digital tools to work more effectively across the public safety system, ensuring we do so in an ethical way to safeguard public trust.
5. **Collaborate with the private sector.** We will strengthen our relationships with the private sector to empower it to appropriately share in public safety responsibilities. The private sector, and the users of its services, have always shared responsibility for elements of public safety and, as technologies become easier and more accessible, there are new ways to safely empower those with an active desire to help.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Interoperability and Policing Stakeholders

Our ambition for policing includes a comprehensive approach to interoperability, where seamless collaboration and information exchange are crucial.

We aim to implement a strong foundation by promoting connectivity standards, forming the bedrock of “foundational interoperability”. This will lay the groundwork for our systems to communicate effortlessly.

Building on this, our vision incorporates “structural interoperability” by embracing Open APIs and data standards. Through these interfaces, we will ensure that our data flows coherently while maintaining its structure and integrity. This step will drive uniformity in data exchange across our operational landscape.

We are dedicated to achieving “semantic interoperability” by establishing a shared vocabulary and data dictionaries. This will greatly improve the accuracy of information exchange for policing systems and also enable a comprehensive understanding and foster more meaningful interactions.

As a pinnacle of our ambition, we recognise the significance of “organisational interoperability”. To this end, the strategy is committed to forging robust data sharing agreements, enhancing collaboration among policing and law enforcement agencies. This collaboration will align efforts, enabling us to operate as a unified front for the safety and security of the communities we serve.

All four layers of interoperability are addressed with the application of resources that are already available to policing. The content of each layer has been reviewed and approved by both the National Standards Assurance Board and the National Technical Design Authority.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

LAW ENFORCEMENT INTEROPERABILITY MODEL

The graphic below shows how each interoperability layer integrates in the policing operating environment with, for example, wider law enforcement and the private sector.

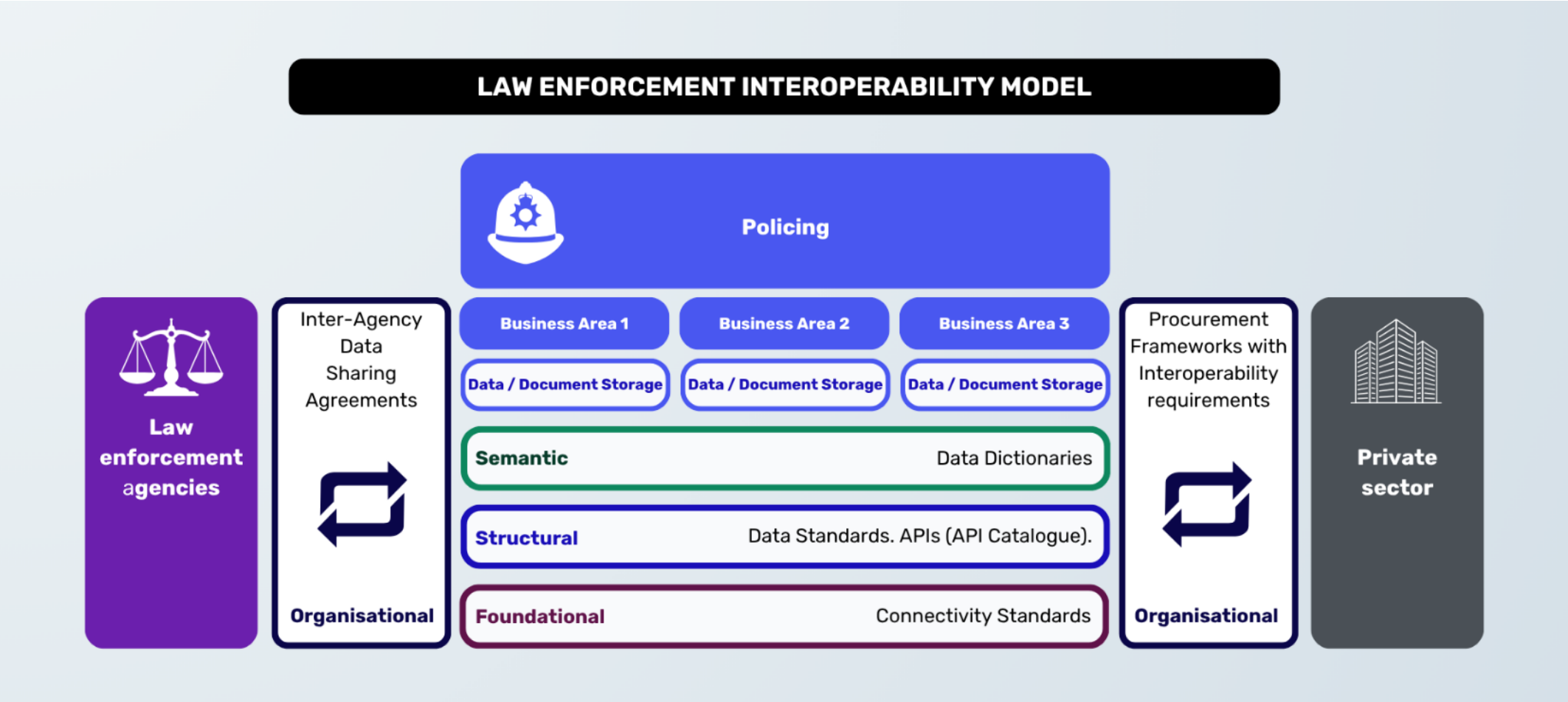


Figure 4 - Interoperability model broken down into the characteristics for each layer

Interoperability reference table

This table offers direct links to resources targeting each level of interoperability. Whether you're building the foundation for data exchange, fine tuning communication protocols, ensuring seamless understanding, or fostering inter-agency collaboration, this table equips you with standards, examples, and insights into improving interoperability.

Level	Standards	Reference material	Examples
Foundational	Frontline Digital Mobility - Connection Types Government network policy changes Frontline Digital Mobility - Portable Hotspots Setup government email services securely ISO/IEC 27033-2:2012 IT Security techniques – Network security Create and iterate an SPF record for email authentication	The OSI Model Government Network Policy Changes Police Box Frontline Digital Mobility Platform	
Structural	POLE data standard OpenAPI Specification	The OpenAPI Initiative JSON XML YAML	JSON Java Script API
Semantic	POLE Data Dictionary The Information Exchange Standard	POLE Data Model	
Organisational	MAIT The Knowledge Hub		

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Review

This policy will be reviewed annually as part of the corporate governance review.

Document Information

Version History

VERSION	AUTHOR	REVISION	DATE
0.1	Brendan Johnston	Initial draft	22/07/23
0.2	PDS	Internal review	10/10/23
0.3	PDS	Internal review	14/04/24
0.4	PDS	Architecture review	24/10/25
1.0	Brendan Johnston/Milan Bollegala	Final Draft	22/04/26
1.1	Brendan Johnston/Milan Bollegala	Internal review	17/07/2026

Consultation

VERSION	NAME	ROLE & Directorate	DATE
0.4	Jo Faulkner	Head of Business Change & Benefits	20/01/26
0.4	TechUK Interoperability Forum	Clare Mosley, Simon Hall, Robert Leach, Paul Daglish, Robin Sanderson	06/02/26

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Approvals

VERSION	AUTHOR	ROLE & DIRECTORATE	DATE
1.0	National Standards Board		29/04/26

Distribution List

VERSION	NAME	ROLE	DATE
1.0	TechUK Interoperability in Justice and Public Safety Forum members	Consultation and advisory group	22/05/26

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL

Core Principles Summary

The core principle of this document is that interoperability is essential to creating a coherent, efficient and data-enabled policing system. It is not presented as a purely technical issue, but as a strategic capability that allows policing, law enforcement partners, criminal justice agencies and suppliers to share information securely, consistently and meaningfully across organisational boundaries. Without interoperable systems, policing risks continued fragmentation, duplicated effort, inconsistent data quality and limited ability to deliver national reform, productivity improvement, AI-enabled analysis and joined-up public safety outcomes.

Interoperability depends on four mutually reinforcing layers. Systems must first be able to connect and exchange data through reliable networks and communication protocols. They must then structure that data using common schemas, message formats, APIs and exchange standards so that systems can process it consistently. Beyond structure, the data must carry shared meaning through common data models, dictionaries, metadata, ontologies and controlled vocabularies. Finally, organisations must align governance, data sharing agreements, responsibilities, assurance processes and decision-making so that information can be shared lawfully, securely and effectively across institutional boundaries.

The document promotes a standards-led approach. Common standards reduce complexity, improve data quality, support integration, enable supplier assurance and create a shared foundation for national policing capabilities. Open and standard APIs, recognised data exchange formats such as JSON and XML, common policing data models such as POLE, and approved national standards are treated as practical mechanisms for moving from local variation to national consistency. Standards should be built into system design, procurement, supplier roadmaps and governance rather than treated as optional add-ons after systems have been deployed.

A further principle is that interoperability should be assessed and improved deliberately. Organisations should understand their current maturity, identify gaps against minimum requirements, set measurable objectives and plan improvements across short, medium and long-term horizons. Foundational and structural capabilities usually need to be established before semantic and organisational interoperability can be achieved. Progress therefore requires a staged journey, supported by clear accountability, realistic resourcing, testing with partner organisations and regular review through existing governance forums.

The document also makes clear that interoperability must be embedded in the wider policing ecosystem. Suppliers should be expected to demonstrate how their products support open or standard interfaces, approved standards, compatible data models, secure transmission, maintainable roadmaps and integration with national platforms. Policing organisations should use shared repositories, national standards platforms, data sharing agreements and existing national boards to coordinate effort and avoid isolated solutions. The overall aim is to make

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL



meaningful information available to the right people, at the right time, in the right form, with appropriate governance and security. In doing so, interoperability becomes a core enabler of reform, operational effectiveness, public trust and long-term digital sustainability.

DATE:	17 July 2026	COPYRIGHT:	
VERSION:	1.0	NUMBER OF PAGES:	38
DOCUMENT REFERENCE:		CLASSIFICATION:	OFFICIAL