POLICE DIGITAL SERVICE

# Technology & Architecture Principles

**VERSION**: 2.0
**DATE**: 7th October 2024
**CLASSIFICATION**: OFFICIAL-FOR PUBLIC RELEASE


**DOCUMENT SIZE**: 18-Page Document

**ABSTRACT:**
These Technology & Architecture Principles are designed to provide Police Digital Service (PDS) with a standard set of general rules and guidelines to inform and guide the procurement, design, delivery, assurance and management of digital services for UK policing.

These principles also serve as a useful reference for local forces, policing bodies, national investment decision makers and those delivering IT solutions for, and on behalf of, UK policing.

| | |
|---|---|
| **ISSUED** | October 2024 |
| **PLANNED REVIEW DATE** | September 2025 |
| **DISTRIBUTION** | National Standards Platform for Policing |

**STANDARDS VALIDITY STATEMENT**
This document is due for review on the date shown above. After this date, principles, standards, and associated guidance may become invalid.

Users should ensure that they are consulting the currently valid version of the documentation.

# DOCUMENT INFORMATION

**Document Location:**

**Revision History**

| Version | Author | Description | Date |
|---|---|---|---|
| 1.0 | Wayne Parkes | First draft – proposed document. | 10.06.21 |
| 1.5 | Scott Adams, Michael Fidler, Brendan Johnston. | Annual update - content reviewed and major updates made. | 20.11.22 |
| 1.6 | Scott Adams | Introduction added. Updated to new PDS document template. Updates from SLT added. | 12.12.22 |
| 1.7 | Michael Fidler, Scott Adams, Anders Lewis | Annual Review – Changes to introduction and 'look and feel'. Core principles unchanged. | 28.09.23 |
| 2.0 | Gavin Morrison | Annual review at Architecture Working Group. Core principles remain the same but wording refined. | 30.09.24 |

**Review and Approvals**

| Version | Name | Role | Date |
|---|---|---|---|
| 2.0 | Gavin Morrison, PDS | Chief Architect – Review with Architecture Working Group | 12.09.24 |
| 2.0 | Andrew Douthwaite, PDS | CTO – Approval | 7.10.24 |

# CONTENTS

# 1. Introduction

"Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission[1]."

These Architecture Principles are designed to support Police Digital Service (PDS) in their delivery of IT services, products and solutions to UK policing. These principles will be used to inform investment decisions and act as a standard framework to guide PDS in the procurement, design, delivery, assurance and management of digital services for UK policing.

These principles are designed to embody the collective strategic digital vision of UK policing, to ensure digital solutions are procured, developed and delivered in line with the National Policing Digital Strategy.

Whilst these principles have been authored to support PDS in the design and delivery of digital services for UK policing, they also serve as a useful reference for local forces, policing bodies, national investment decision makers and those delivering IT solutions for, and on behalf of, UK policing. Alignment to these principles can help drive a more consistent approach to digital delivery across the wider UK policing landscape. This in turn can help provide a collective drive towards delivery against the National Policing Digital Strategy.

These Architecture principles will be published openly on the Internet via the 'National Standards Platform for Policing'. This will not only enable easy consumption by those within UK policing, but will also help guide and empower the private sector, to help them deliver solutions that meet the needs and strategic ambitions of UK policing.

# 2. Structure of Architecture Principles

In keeping with The Open Group Architectural Framework (TOGAF) and other similar architectural frameworks, the principles described within this document will be structured in the following way:

| | |
|---|---|
| **Name:** | Should both represent the essence of the rule as well as be easy to remember. |
| **Statement:** | Should succinctly and unambiguously communicate the fundamental rule. |
| **Rationale:** | Explanation of why the principle is important and how it will benefit policing and law enforcement organisations. |
| **Implications:** | In the form of a list to describe what is required to successfully carry out the principle and how it could potentially impact the organisations and those who supply to them. |

[1] The TOGAF Standard, Version 9.2 - Architecture Principles (opengroup.org)

## 3. Principles

Organisations and individuals should ensure alignment to these Architecture Principles when making investment decisions or designing, delivering, assuring or managing digital solutions/services on behalf of UK policing.

# Principle 1: National strategic fit

**Statement:** Solutions will strengthen, enhance and/or enable delivery of the National Policing Digital Strategy (Digital, Data and Technology Strategy 2020-2030).

**Rationale:** PDS and policing organisations need to deliver against strategic ambitions, ultimately to deliver improved UK policing services.

**Implications:**

- Strategic fit is a key determining factor when assessing solutions.
- A gated review process will be established to ensure solutions are strategically aligned, and their investment is strategically beneficial, governed by a central strategic prioritisation board.
- Policing and their suppliers need to support the national strategic vision.
- Commercial-off-the-shelf (COTS) products will be favoured over bespoke solutions.
- Cloud-first solutions and managed services will be favoured over self-hosted, self-managed solutions. These will be fully evaluated to ensure strategic fit, as well as suitability and legal compliance for the data to be hosted. 05/06/2025

# Principle 2: Maximise policing outcomes

**Statement:** Solutions will be designed or selected with a view across the whole of the UK policing landscape to add, enhance or maintain valued and trusted services to UK policing.

**Rationale:** By taking a holistic view to realise the full suite of potential benefits and opportunities for UK policing, including at a regional and national level, solutions can seek not only greater economies of scale and efficiencies, but can also take steps to drive a more joined-up and improved police service.

**Implications:**

- The formation of an Enterprise Architecture function providing coordination, governance, control and leadership. This needs to be in place within PDS for, and on behalf of, UK police forces. The function will follow EA best practice and make use of industry standard frameworks and tooling.
- Need a centrally accessible national register of technology solutions that exist, are under development or are being proposed.
- Clear leadership, shared ownership, and a joined up approach to delivery will be encouraged, which in turn will inform technical decision making.

# Principle 3: Benefits are measurable and maximised

**Statement:** Benefits will be defined and agreed in advance in a manner that are both measurable and demonstrable.

**Rationale:** Agreeing benefit measures upfront provides greater clarity and transparency as to whether benefits have actually been delivered during the product lifecycle. By recording benefits at the time of their realisation, not only does this provide for more accurate reporting, but also saves time in retrospectively trying to attribute benefits. Regular review of these benefits can then be used to maximise the potential of the solution and support wider future investment strategies.

**Implications:**

- Benefits need to be considered at the start of any project.
- Benefits and their measures will be agreed and accepted by those accountable in advance of authority to proceed.
- Automated or simplified benefits measurements should be used wherever possible.
- Suitable tooling needs to be available to track benefits.
- Benefits measures need to be incorporated, where practicable, into supplier and/or service contracts.
- Regular benefits reports need to be produced at an agreed frequency to report to key stakeholders.
- Business cases which do not properly state the benefits and their measures will supported.

# Principle 4: Problem statements are well defined

**Statement:** Solutions are designed and assessed against one or more problem statements, that have been fully defined, agreed and prioritised.

**Rationale:** In order to deliver the best possible solutions that take into account wider strategic ambitions, solutions should not be delivered in a reactive, resolution-driven fashion. Solutions should instead be delivered in a way that demonstrably addresses specific and well-defined problems, supported by strong governance and gate reviews, to ensure solutions meet both the current and future needs of UK policing.

**Implications:**

- Stakeholders should approach technologists with clearly defined problem statements not with pre-formed solutions.
- Problem statements will be prioritised based on an agreed and objective prioritisation framework.
- Solutions will be designed or selected based on well-articulated problem statements and their relative priorities.

# Principle 5: Requirement-led design

**Statement:** Functional and non-functional requirements will be captured in a manner that allows a varied range of end-users to clearly articulate and define what they need.

**Rationale:** In order to design solutions that best meet the needs of UK policing, requirements of users from multiple perspectives need to be taken into account both prior to and during the design and selection. This ensures solutions are designed or selected with the needs of the service users (both current and future) at the heart of delivery.

**Implications:**

- User requirements are accurately captured and included in solution design using proven methodologies, such as user stories, use cases and problem statements.
- Requirements will be captured from a full range of perspectives relevant to the solution, for example: Frontline Officers; Senior Officers; Home Office; College of Policing; General Public; Human Resources; Facilities; Information Technology; Information Management etc.
- Solutions should seek to capture and enable future (strategic) requirements. Eg: Improved future interoperability; Improved data-sharing; hands-free interaction etc.
- Solutions must take into account accessibility and adhere to the prevailing accessibility regulations.

# Principle 6: Simple and scalable

**Statement:** Complex solutions will be simplified and delivered following an agile, iterative approach to deliver benefits quickly and incrementally. Solution design will follow a cloud first approach with a view to national scale and reuse across Law Enforcement and partners.

**Rationale:** Delivering complex, large-scale projects following a big bang or waterfall approach tends to result in a higher rate of failure and slower delivery of value to the end user. Industry best practice is to deliver complex IT projects in an agile and incremental manner, with regular and meaningful stage gate reviews. This enables timely decision making, faster return on investment, and improved benefits realisation.

**Implications:**

- The funding models need to reflect the change to a more flexible delivery methodology, and move away from one-off programme funding.
- Governance models need to be in place to support regular feedback, regular review and regular decision making. (This includes the need for delegated decision making).
- Where appropriate, solutions need to be designed to scale locally, regionally, and nationally.
- Projects must embed timely decision making, an ability to change direction, and a willingness to acknowledge failure (fail fast philosophy).
- Solutions need to be designed with future change in mind.

# Principle 7: Reduce duplication, increase re-use

**Statement:** Solutions should aim to reduce the levels of duplication within the policing technology estate and should reuse existing products, components and shared services where possible.

**Rationale:** Reuse of existing products, components and services improves time to first value and return on investments. Reducing duplication of services and solutions across the technology estate can deliver cost efficiencies and drive further simplification and convergence.

**Implications:**

- There needs to be a good understanding of the existing policing landscape to identify duplication and opportunities for reuse. (Enterprise Architecture capability)
- Solutions should adopt or align with National Standards and guidance.
- Solutions should be interoperable and support API integrations.
- Data should be re-used, taking advantage of the golden nominal concept and common data standards.

# Principle 8: Digital First

**Statement:** Solutions enhance user experience by exploiting digital services, automation, accessibility and mobility. They remove the need for physical media, such as removable media and paper documents. Service users can complete tasks digitally, end-to-end, from authorised devices and/or authorised locations.

**Rationale:** The digital-first approach ensures that solutions and services are designed as digital-by-default, with user experience, process efficiency and data management at the core of their creation. This enables solutions to utilise the full potential of digital services, to deliver maximum benefit to the user, organisation and UK policing.

**Implications:**

- Business processes and management of police information may need to be reviewed and redesigned to remove the requirement for physical media.
- Criminal Justice implications need to be carefully considered, e.g. requirements for evidential material and data sharing with criminal justice partners.
- Solutions are designed from the end-user's perspective (see Principle 5).
- Integration with other systems and data sets should be considered from the outset to ensure solutions and services are truly digital-first, from end-to-end.

# Principle 9: Compliant

**Statement:** Solutions and services must comply with all relevant laws, policies, regulations, standards, and guidance.

**Rationale:** Compliance decreases information security and operational risk, and can positively impact core policing operations. Building solutions that are aligned from the outset can reduce costs and deliver outcomes that are more closely aligned with requirements. Non-compliance can increase cost and lead to significant operational, financial and reputational damage, and put at risk core policing duties, impact the ability to secure successful convictions, and even pose a threat to life.

**Implications:**

- The appropriate and relevant level of compliance needs to be understood and agreed at the beginning of the commissioning process.
- An upfront assessment of the business, data, technology, security, and environmental impacts of the solution will help inform the relevant compliance requirements.
- Changes in compliance requirements may drive changes to solutions, services and processes. It is essential that these are well managed and monitored, and that the solution is suitably adaptable, to ensure ongoing compliance.
- Robust governance and assurance processes must be instituted to ensure continuous compliance.

# Principle 10: Sustainable change

**Statement:** Solutions and services are designed to be adaptable to enable ongoing business change.

**Rationale:** Change in modern policing is accelerating, and solutions, services and their underpinning commercial agreements need to reflect this. Business agility is key. Services must be extensible and adaptable to meet the needs of UK policing and its users, whilst being portable through use of common technologies and data abstraction to minimise and avoid vendor lock-in.

**Implications:**

- Non-functional requirements will be defined for sustainable change, including extensibility, interoperability, maintainability, and portability requirements.
- Need to build in commercial terms to support business agility through flexible supplier contracts and partnerships agreements.
- Support and ongoing Service Level requirements need to be fully understood and delivered through agreed SLA's.
- Solutions must be delivered with products that benefit from ongoing and available support.
- Configuration is preferred over customisation, to reduce complexity, making it easier to manage, update and support services.
- Open standards, common standards, and industry best practises shall be adopted to avoid vendor lock-in.
- Exit strategy and data migration will be defined and understood from the offset, to further reduce vendor lock-in / complexity to migrate to another vendor.
- The cost of sustainability requirements such as extensibility and portability will be managed and considered when developing or procuring a new system.

# Principle 11: Secure by design

**Statement:** Solutions will be developed following a secure by design approach, embedding security, privacy, and resilience from inception, through to final delivery, and ongoing business-as-usual activities.

**Rationale:** Building secure solutions with security embedded from the outset is shown to result in reduced cost, time and risk, rather than trying to retrospectively re-engineer, re-architect or reconfigure systems to try to meet security requirements after the event.

**Implications:**

- Following a secure by design approach helps ensure security, privacy and resilience considerations are factored in from the outset.
- The PDS Cyber Service and other security stakeholders will be actively engaged from the outset to shape the cyber security requirements.
- Solution design will need to balance security requirements with user-requirements, which may at times conflict.
- Solutions must be architected in alignment with the PDS Cyber Security Architectural Principles to ensure a consistent approach.

# Principle 12: Interoperability and better use of data

Statement: Policing systems should be interoperable and should enable the safe and secure sharing of data without manual intervention or bespoke configuration.

Rationale: Policing data is a valued and essential asset. Increased interoperability and the ability to seamlessly share data between systems opens-up significant opportunity for UK policing. This ranges from enabling data sharing across criminal justice partners; reduction of double-keying; reduced time and cost to implement new solutions, including use of COTS products; greater agility to implement new and innovative solutions; greater ability to connect with the UK public to provide a 'seamless citizen experience'.

Implications:

- Interoperability and better use of data should be considered from the outset of any project, including wider engagement with the private sector and public sector data bodies.
- Solutions should conform to National Standards, including APIs standards and shared data dictionaries.
- Where existing National Standards don't exist, and a system is being developed where interoperability is likely, the National Standards team should be engaged early on to evaluate whether a standard can be developed, or an existing standard adopted.
- Access to data should be controlled and managed through nationally established capabilities, such as the National Identity and Access Management (NIAM) solution.
- Solutions should provide secure data-sharing capabilities by default and adhere to relevant national data principles.