| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 24-2299Responded to: 04 October 2024 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## Data Governance - Does your police force have a documented data governance framework? (Yes/No)

Yes.

## If yes, when was it last reviewed and updated?

I can confirm it was last reviewed and updated in July 2024.

## Data Leadership - Is there a designated Chief Data Officer (CDO) or equivalent role within your police force? (Yes/No)

Yes.

## How many Full-Time Equivalent (FTE) staff are dedicated to data management and analytics? Please break this down by Data Analysts, Data Scientists, Data Engineers, Data Architects, Database Administrators & Data Leaders.

Within the Chief Data Office, there are 54 full time employees. This excludes Data Analysts and Database Administrators who are spread across all divisions within Police Scotland.

## Data Quality Management - Does your force routinely (at least quarterly) assess the quality of its data (e.g., accuracy, completeness, timeliness)? (Yes/No)

Yes, there is an Enterprise Data Quality Team established within the Chief Data Office as of June 2024.

## What percentage of your force's critical datasets have been subject to a formal data quality assessment in the last year?

Zero, the Data Quality Team was only established alongside new Data Governance Framework in July 2024. Formal data quality assessment will be carried out when critical data elements are established through the data governance framework.

## Data Strategy - Is there a data strategy aligned with your force’s broader organizational strategy? (Yes/No)

## Please provide the year when the data strategy was first implemented and any subsequent revisions. Please also provide the strategy document if available.

Yes, the data strategy is part of the organisations 2024 Digital Strategy, which can be viewed online - [Digital Transformation - Police Scotland](https://www.scotland.police.uk/about-us/how-we-do-it/strategic-planning/digital-transformation/).

Prior to this the data strategy has informed the Data Drives Digital Programme, the organisations strategic change programme for data.

## Data Literacy - Has your force implemented any formal data literacy programs or training for staff? (Yes/No)

No.

## What percentage of your staff have completed data literacy training in the last 12 months?

Zero, however, data literacy forms a module within the College of Policing’s Strategic Command Course that all senior officers must undertake.

## Data Infrastructure and Technology - What data management platforms or tools does your force use (e.g., data warehouses, ETL tools, analytics platforms)?

I am refusing to confirm or deny whether the information sought exists or is held by Police Scotland in terms of section 18 of the Act.

Section 18 applies where the following two conditions are met:

- It would be contrary to the public interest to reveal whether the information is held

- If the information was held, it would be exempt from disclosure in terms of one or more of the exemptions set out in sections 28 to 35, 38, 39(1) or 41 of the Act.

If the above data was held, the following exemptions would be considered relevant:

**Section 31(1) - National Security and Defence**

Information is exempt information if it is required for purpose of safeguarding national security.
Disclosure would undermine any ongoing or future operations to protect the security or infrastructure of the United Kingdom and increase the risk of harm to the public. It is important to note that the UK faces a serious and sustained threat from violent extremists and this threat is greater in scale and ambition than any terrorist threats in the past.

**35(1)(a)&(b) – Law Enforcement**

Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice substantially the prevention or detection of crime and the apprehension or prosecution of offenders.
Disclosure would assist groups, organisations and those with hostile intent to identify, with some accuracy, Police Scotland’s technological capabilities and take steps to attack or hijack known vulnerabilities to Police systems directly or the supply chain.
Disclosure would assist those with intent on doing harm with a tactical advantage when planning or perpetrating criminal plans and unlawful activities, and maximise the impact of destruction, harm and disruption that may be caused.

**Public Interest Test**

Public accountability may favour disclosure, given that the information concerns the efficient and effective use of resources by the Service. Likewise, disclosure of the information would also inform the public debate on the issue of policing and technology and contribute to the accuracy of that debate.
Conversely, the need to ensure the effective conduct of the service in relation to prevention and detection of crime and the maintenance of national security clearly favour non-disclosure of the information requested.
Accordingly, I would argue that the public interest lies in favour of non-disclosure of the information requested.

## Does your force have a cloud strategy for data storage and processing? (Yes/No)

No.

## Data Sharing and Integration - To what extent does your force share data with other forces and public sector bodies? (Scale: None, Limited, Extensive)

Extensive.

## Does your force have standardized protocols for data integration between internal systems? (Yes/No)

Yes, we use the following:

Microsoft Structured Query Language Server Integration Services

Open Database Connectivity

Java Database Connectivity

Microsoft Message Queue

Representational State Transfer Application Programming Interface

## Data Ethics and Privacy - Does your force have an ethics board or similar body that reviews data-related projects? (Yes/No)

Yes, the force has a Data Ethics strategy and framework that includes a Data Ethics Oversight Group (currently in ‘trial phase’) and an independent Data Ethics Group.

## Are there policies in place to ensure data privacy compliance (e.g., UK GDPR, UK DPA)? (Yes/No) If yes, please list the data privacy policies you follow and adhere to.

Yes, Data Protection, Information Security, Intelligence Data and Records Management.

These are available online - [Policies and Procedures - Police Scotland](https://www.scotland.police.uk/access-to-information/policies-and-procedures/)

## Data Use and Analytics - What proportion of your force's operational decisions are data-driven? (Please estimate a percentage)

The information sought is not held by Police Scotland and section 17 of the Act therefore applies. Information is not held in this format and we are unable to quantify.

## Does your force use widespread (across multiple departments) advanced analytics (e.g., predictive modelling, AI, machine learning) to inform policing strategies and crime prevention? (Yes/No)

No.

## Continuous Improvement and Innovation - Does your force have a process for continuously improving its data management practices? (Yes/No)

Yes.

## How often are new data management technologies or practices piloted within your force?

The information sought is not held by Police Scotland and section 17 of the Act therefore applies. Information is not held in this format and we are unable to quantify.

If you require any further assistance, please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.