

# Staffordshire Police

## Data protection audit report

November 2024

# Executive summary

---



## Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and other data protection legislation. Section 146 of the DPA 2018 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA 2018 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

Staffordshire Police (SP) agreed to a consensual audit of its data protection practices.

The purpose of the audit is to provide the Information Commissioner and SP with an independent assurance of the extent to which SP, within the scope of this agreed audit, is complying with data protection legislation.

The scope area covered by this audit was determined following a risk based analysis of SP's processing of personal data. The scope may take into account any data protection issues or risks which are specific to SP, identified from ICO intelligence or SP's own concerns, or any data protection issues or risks which affect its specific sector or organisations more widely. The ICO has further tailored the controls covered in the scope area to take into account the organisational structure of SP, the nature and extent of SP's processing of personal data. As such, the scope of this audit is unique to SP.

It was agreed that the audit would focus on the following area:

| Scope area   | Description  |
|--|--|
| <b>Personal data breach management and reporting</b> | The extent to which SP has measures in place to detect, assess and respond to security breaches involving personal data, to record them appropriately and notify the supervisory authority and individuals where appropriate |

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, remote interviews with selected staff, and a virtual review of evidential documentation.

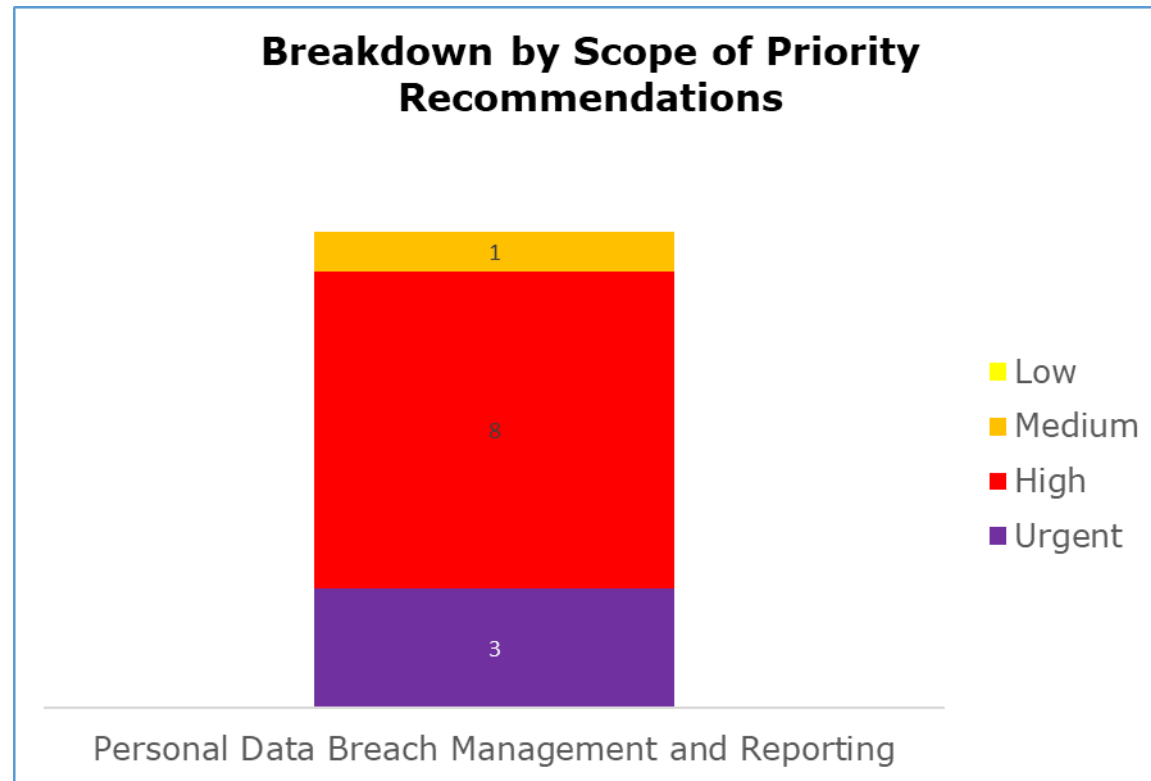
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist SP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. SP's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

## Audit Summary

| Audit Scope area                              | Assurance Rating | Overall Opinion   |
|---|------------------|---|
| Personal Data Breach Management and Reporting | Limited          | There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation. |

The assurance rating above is reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

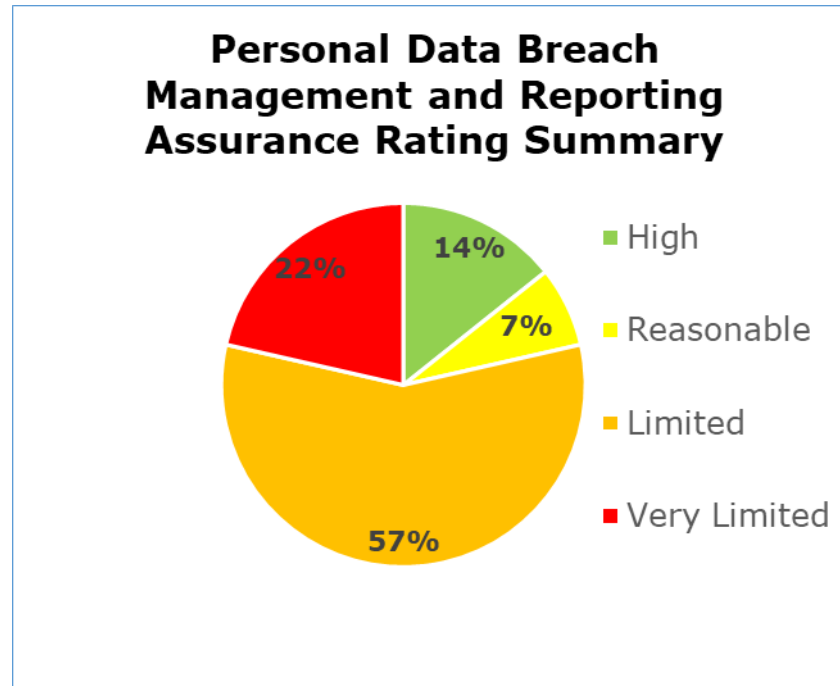
## Priority Recommendations



The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Personal data breach management and reporting has three urgent, eight high and one medium priority recommendation.

## Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the personal data breach management and reporting scope. 14% high assurance, 7% reasonable assurance, 57% limited assurance, 22% very limited assurance.

## Key areas for improvement

We identified some key areas within our audit, where SP needed to implement further measures to comply with data protection law.

- SP should assess the resources in the Information Assurance Department and ensure that it is adequately resourced to manage their responsibilities in preventing and responding to any suspected personal data breaches (PDBs). This includes the Data Protection Officer (DPO) and their statutory tasks.
- Regular refresher data protection training should be mandated across the force which includes awareness of SP's breach reporting processes and what should be reported.
- Regular specialist training should be provided to all staff who are involved in decisions about potential PDBs.
- The out of hours reporting processes should be reviewed to provide assurance that PDB's will be appropriately handled whenever they are reported.
- Data flow mapping should be completed to identify any data sharing arrangements which require formal agreements to specify how any PDBs should be managed.

## Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance, and internal control arrangements in place rest with the management of Staffordshire Police.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting, or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Staffordshire Police. The scope areas and controls covered by the audit have been tailored to Staffordshire Police and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.