# Kent Police

## Data protection audit report

October 2022

Information Commissioner's Office

# 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 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 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.

Kent Police (KP) agreed to a consensual audit of its processing of personal data. An introductory telephone meeting was held on 11 July 2022 with representatives of KP to discuss the scope of the audit.

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

The scope areas covered by this audit are determined following a risk based analysis of KP processing of personal data. The scope may take into account any data protection issues or risks which are specific to KP, identified from ICO intelligence or KP own concerns, and/or any data protection issues or risks which affect their specific sector or

organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of KP, the nature and extent of KP processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to KP.

It was agreed that the audit would focus on the following area(s)

| Scope area | Description |
|---|---|
| **Records Management** | The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records. |
| **Requests for Access** | There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data. |

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.

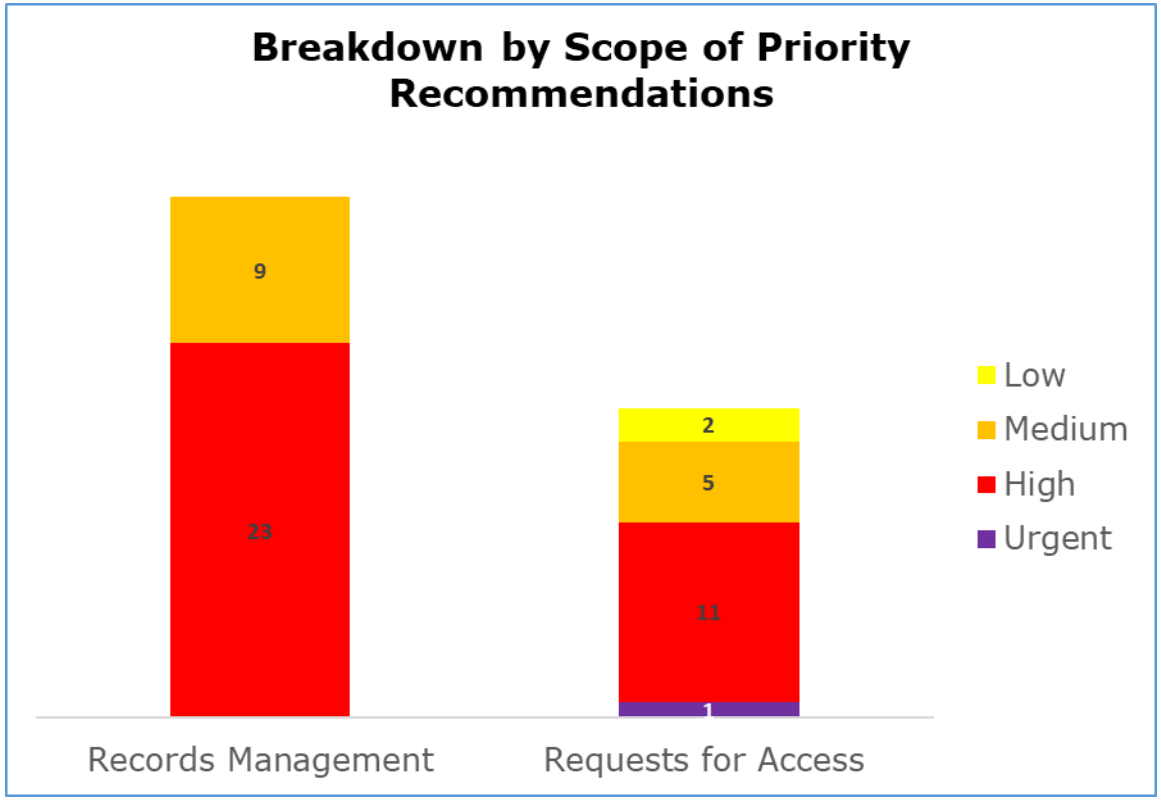
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist KP in implementing the recommendations each has been assigned a priority rating based upon the risks that they are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

The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

# Audit Summary

| Audit Scope area | Assurance Rating | Overall Opinion |
|---|---|---|
| **Records Management** | 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. |
| **Requests for Access** | 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. |

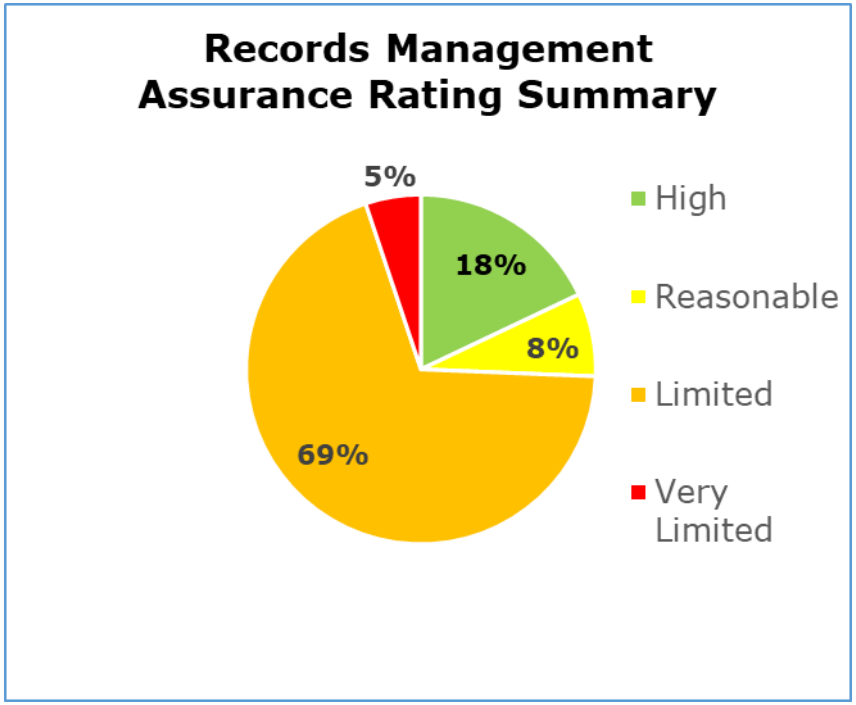
## Priority Recommendations



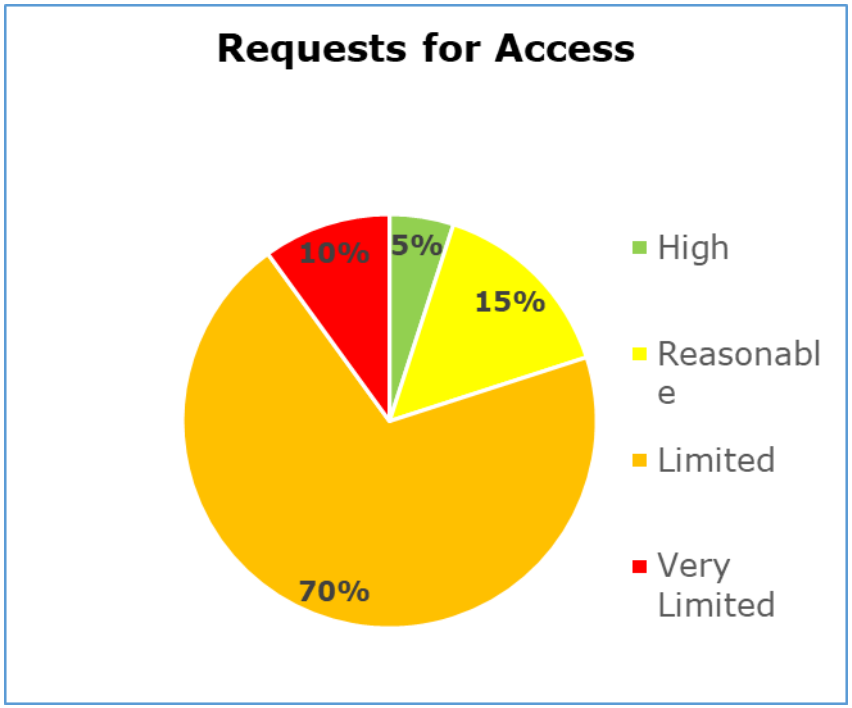

The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Records Management has 0 urgent, 23 high, 9 medium and 0 low priority recommendations.
- Requests for Access has 1 urgent, 11 high, 5 medium and 2 low priority recommendations.

## Graphs and Charts




The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 18% high assurance, 8% reasonable assurance, 69% limited assurance, 5% very limited assurance.




The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 5% high assurance, 15% reasonable assurance, 70% limited assurance, 10% very limited assurance.

## Areas for Improvement

Continuation of the recruitment of a Records Manager and Assistant Records Manager will ensure there is sufficient operational responsibility in place for the development and implementation of the RM function.

The completion of a Training Needs Analysis (TNA) will strengthen the DP training programme and help KP to assess what additional aspects of RM should be included within both the induction and annual refresher training and will highlight specialised training requirements. The content of both training packages should link into the RM policy framework.

Ensure all policies and procedures which have been drafted for the use of SharePoint (SP) are ratified, approved and communicated to all staff across the organisation who are currently using SP as an Electronic Discovery Reference Model (EDRM).

The completion of an information audit (data mapping) for all departments will ensure that all information assets have been identified and recorded. This will assist KP in the development of their Information Asset Register (IAR)/Record of Processing Activities (ROPA).

Conducting a gap analysis of the current IAR/ROPA template will help KP to assess what information is required under Article 30 of the UKGDPR and Section 61 of the DPA18 and understand what is currently missing and what must be recorded.

Continue to review the backlog of the Management of Police Information (MOPI) graded files to ensure retention periods continue to apply. Securely dispose of records which have fallen outside of their retention period.

KP should continue to monitor the number of staff in place, to ensure the level of resource is sufficient to be able to handle incoming requests for access whilst also working through the existing backlog.

When responding to a request for personal data the required supplementary information must be provided alongside copies of the personal data requested. This must be sufficiently granular and specific to the data subject that made the request to ensure compliance with Article 15 of the UKGDPR and Section 45 of the DPA18.

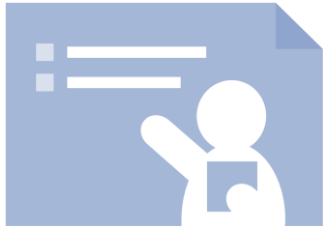
The implementation of a formal approval process would help to ensure that proper consideration is given and documented to the removal of personal and third party data that is exempt from disclosure. Furthermore, the creation of a quality assurance process would ensure a consistent approach to the application of exemptions and the removal of personal and third party data, across the Public Disclosure Team (PDT).

KP should continue to review the processes adopted by the public disclosure team, especially those involving Body Worn Video, to improve compliance with statutory timescales in responding to subject access requests (SARs).

KP should ensure that the compliance with statutory timescales for SARs is discussed regularly at the Force Information Security Committee to drive improvement.

KP should document a process for the SAR PDT to incorporate checks with data processors, to ensure all personal data is included in the response to a SAR.

# Appendices



**Appendix One** – Recommendation Priority Ratings Descriptions

| |
|---|
| **Urgent Priority Recommendations** -<br>These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation. |
| **High Priority Recommendations** -<br>These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation. |
| **Medium Priority Recommendations** -<br>These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced. |
| **Low Priority Recommendations** –<br>These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion. |

## 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 Kent 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 Kent Police. The scope areas and controls covered by the audit have been tailored to Kent Police and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.