Age UK Wiltshire

Data protection audit report

April 2023

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.

Age UK Wiltshire (AUKW) requested an audit from the ICO in January 2023 and submitted an audit questionnaire detailing their data protection compliance concerns. ICO audit team managers completed a scoping call with AUKW to further discuss their current data protection compliance levels and the appropriate scope areas on which to focus the audit.

The purpose of the audit is to provide the Information Commissioner and AUKW with an independent assurance of the extent to which AUKW, 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 AUKW processing of personal data. The scope may take into account any data protection issues or risks which are specific to AUKW, identified from ICO intelligence or AUKW's 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 AUKW, the nature and extent of AUKW's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to AUKW.

It was agreed that the audit would focus on the following areas.

Scope area	Description
Governance and Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
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.

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.

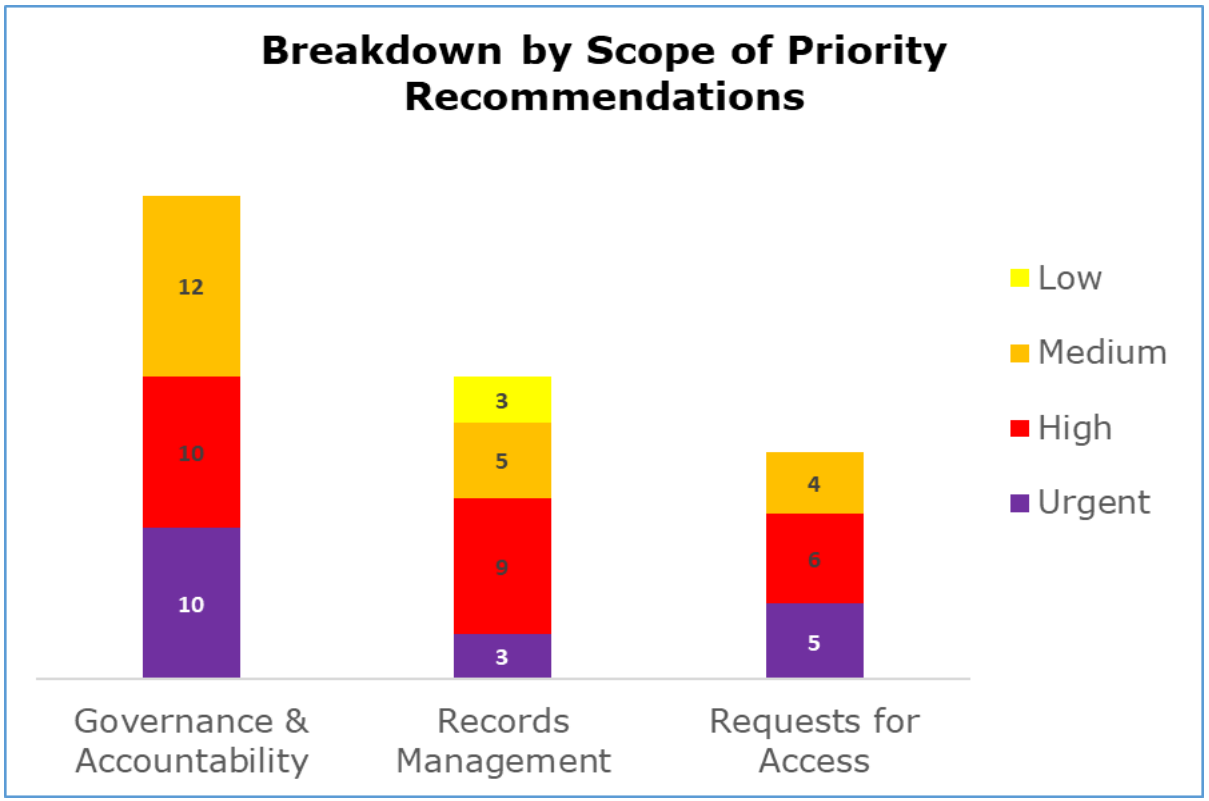
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist AUKW in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. AUKW'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
Governance and Accountability	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.
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	Very Limited	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

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

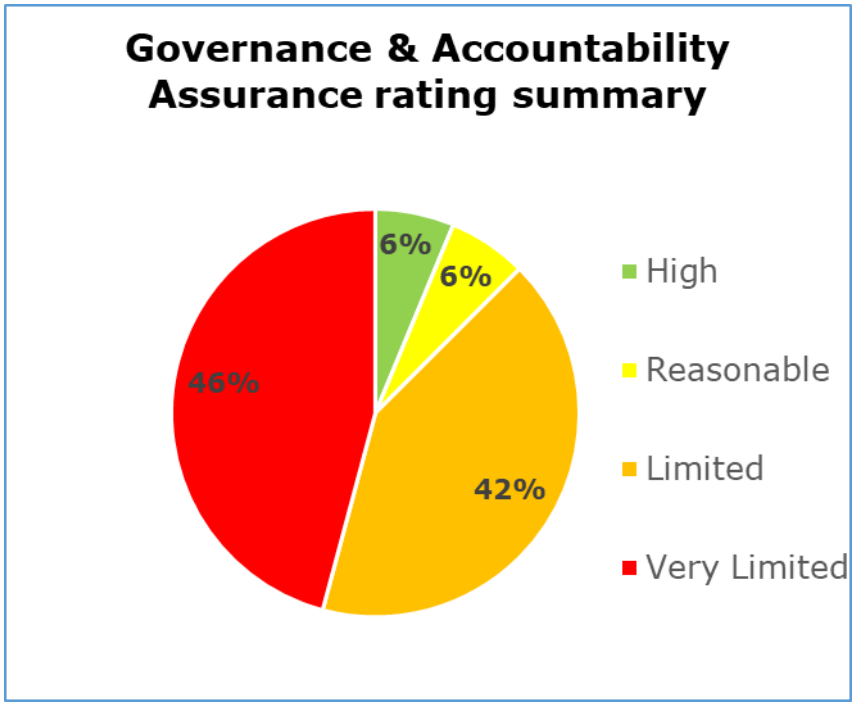
Priority Recommendations



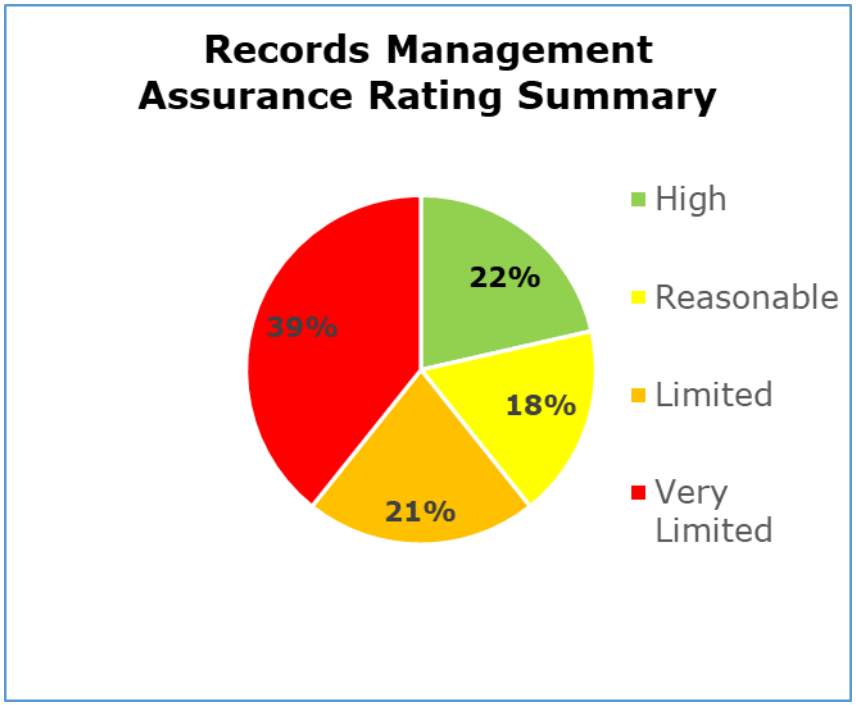
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has 10 urgent, 10 high and 12 medium priority recommendations.
- Records Management has 3 urgent, 9 high, 5 medium and 3 low priority recommendations.
- Requests for Access has 5 urgent, 6 high and 4 medium priority recommendations.

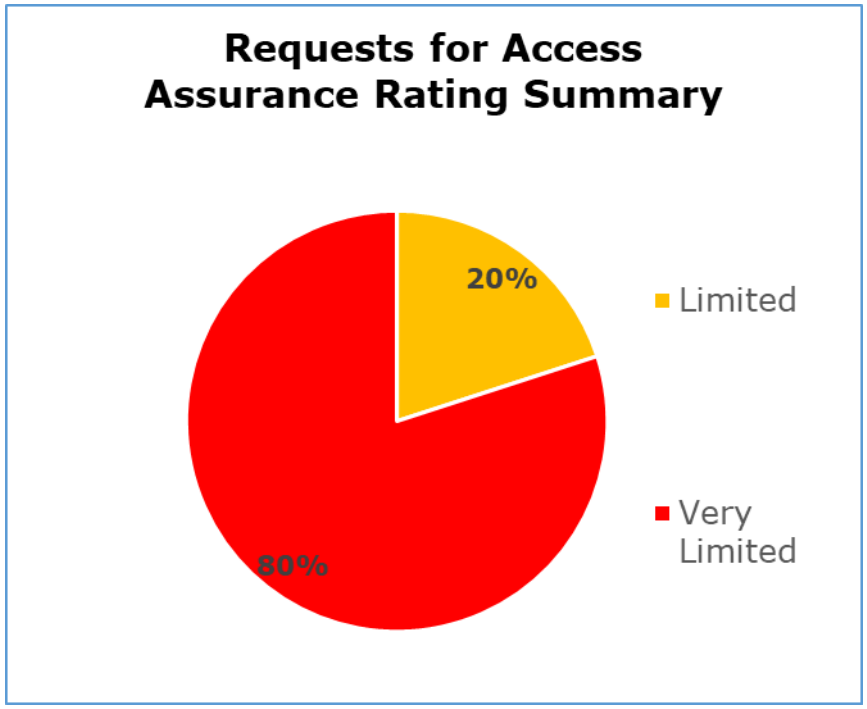
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 6% high assurance, 6% reasonable assurance, 42% limited assurance, 46% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 22% high assurance, 18% reasonable assurance, 21% limited assurance, 39% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Requests for Access scope. 20% limited assurance, 80% very limited assurance.

Areas for Improvement

Governance and Accountability:

Review and update existing data protection policies and create separate new policies covering records management, data sharing, data protection impact assessments (DPIA), and information security.

Ensure the data protection training programme is mandatory for all staff, includes annual refresher training and specialised training for staff in information governance roles.

Carry out regular internal data protection and information governance audits, sufficiently detailed for the context of AUKW, to gain assurance that AUKW's risk management is effective.

Complete an information audit to help AUKW have an understanding of all of the information that is held and how it flows across AUKW. After completing a comprehensive information audit, create a centralised Record of Processing Activities (ROPA) document that demonstrates that AUKW has adequately recorded essential information regarding all of their personal data processing activities.

Records Management:

AUKW should create an Information Asset Register (IAR) to record the information assets identified by the information audit and ensure that the IAR is periodically reviewed and that each asset is risk-assessed, so that high-risk assets can be identified and addressed as necessary to enable AUKW to demonstrate that they have identified and risk-assessed the information they hold.

Create a policy which sets out the arrangements for the access to, and security of electronic records. The policy should include detail on how access permissions for staff members will be determined, and details of the technical measures in place to keep electronic records secure.

Requests for Access:

Continue with plans to review and update the current Subject Access Requests (SAR) guidance including creating an in-depth SAR policy that is communicated to staff and regularly reviewed and updated accordingly.

Create guidance on completing identity checks and include it in the SAR policy.

Create and maintain a SARs log as a documented record of all completed and ongoing SARs. For internal SARs create and maintain a separate log with restricted access to protect the privacy of staff members.

Ensure that all staff are aware of the statutory timeframe for all SARs received and the process they should follow if an extension is required.

Best Practice

Records Management:

Well thought-out security measures were observed within AUKW's Meals Service. Delivery drivers working within the Meals Service carry a route sheet with them which lists the delivery addresses and also includes additional, necessary information relating to clients. This can include codes to key safes, so that the delivery driver can enter clients' properties without needing the client to come to the door. To mitigate the risk of unauthorised access to this information, through the loss of a route sheet or otherwise, key safe codes are encrypted using a cipher. The cipher is available to the drivers, if necessary, within a password protected documented on their password protected work phones.

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 Age UK Wiltshire.

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