University of Chichester (Multi) Academy Trust

Data protection audit report

August 2024

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 (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.

University of Chichester (Multi) Academy Trust (the Trust) requested a consensual audit of its data protection practices. The audit was requested by their recently appointed Data Protection Officer (DPO) as a way of revisiting the Trust's data protection framework, policies and procedures, as there has been significant change of personnel within their central team. The Trust plan to use the findings from the audit to address areas of risk, in order to improve their data protection compliance.

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

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

Scope area	Description
Governance & 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.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

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.

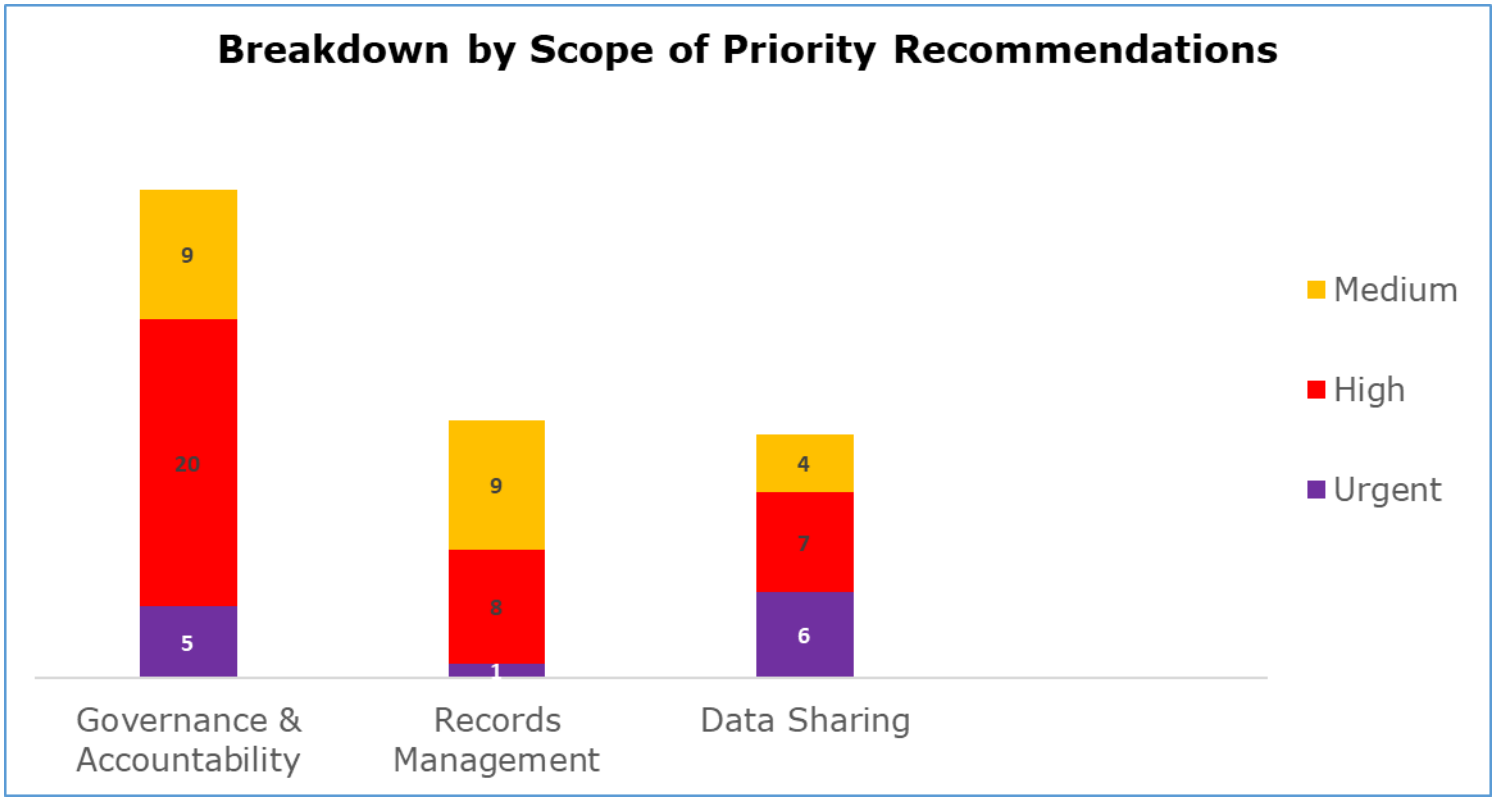
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Trust in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. The Trust'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 & 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.
Data Sharing	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.

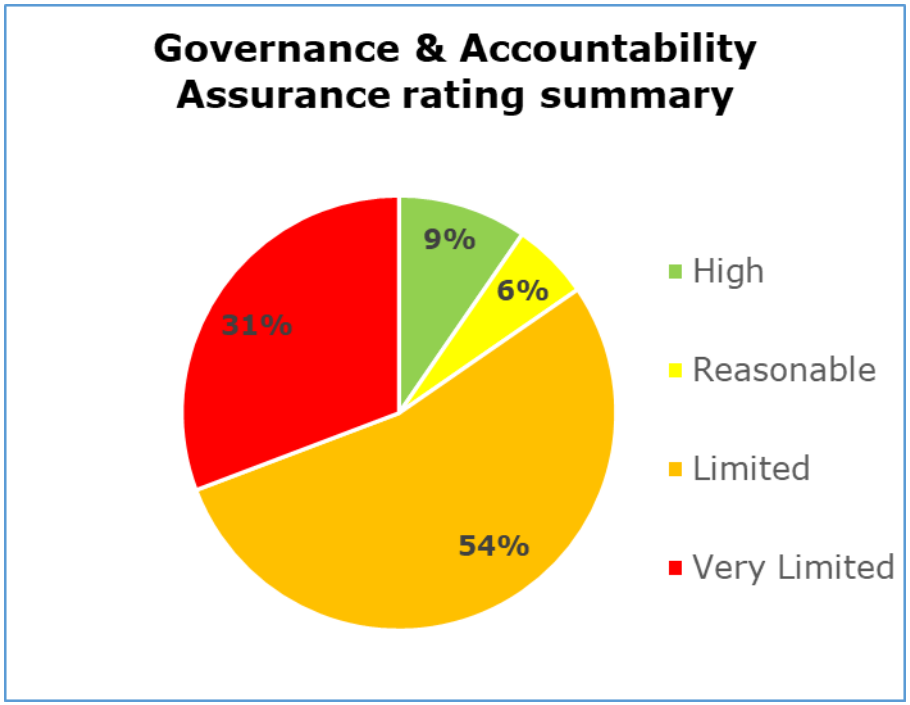
Priority Recommendations



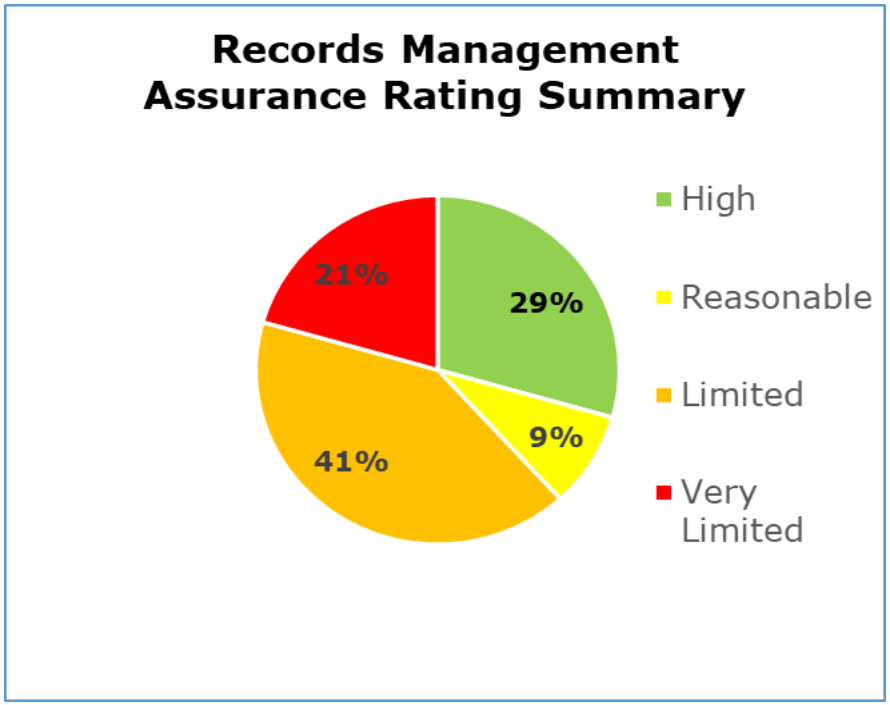
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has five urgent, 20 high and nine medium priority recommendations
- Records Management has one urgent, eight high and nine medium priority recommendations
- Data Sharing has six urgent, seven high and four medium priority recommendations

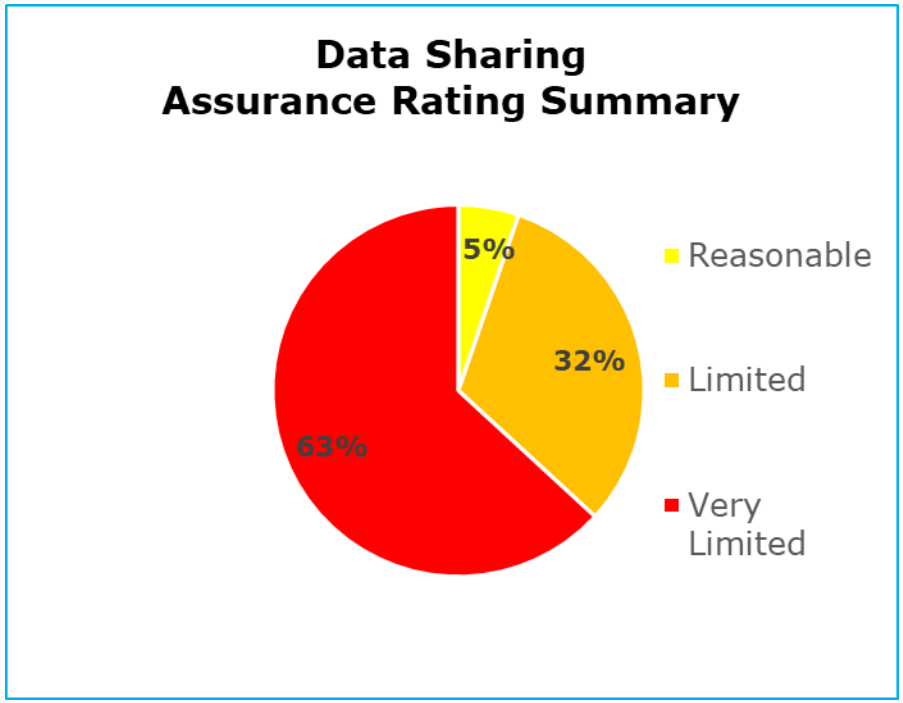
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 9% high assurance, 6% reasonable assurance, 54% limited assurance, 31% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 29% high assurance, 9% reasonable assurance, 41% limited assurance, 21% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. No high assurance, 5% reasonable assurance, 32% limited assurance, 63% very limited assurance.

Areas for Improvement

Governance and Accountability

- The Trust must complete a comprehensive training needs analysis (TNA) to inform their training plan and to identify all the roles that require additional data protection (DP) training. If there is no specialised training provided to key roles, breaches may be caused by lack of specialist knowledge.
- The Trust must create a centralised record of processing activities (ROPA) document to ensure compliance with Article 30 of the UK GDPR. The ROPA should be reviewed regularly to ensure it stays accurate and up to date.
- The Trust must create a documented data protection impact assessment (DPIA) process that enables staff to understand the types of processing that requires a DPIA. This will ensure that DPIAs are always carried out when they should be.

Records Management

- The Trust's retention schedule does not include the storage periods for all records it holds and manages. This risks personal data being retained for longer than necessary and non-compliance with the storage limitation principle of the UK GDPR.
- Not all systems used by the Trust make exhaustive privacy considerations. This could lead to appropriate technical measures not being implemented in all instances.
- The Trust has not formalised its expectations for compliance checks of the physical records held across its different locations. Whilst staff take a diligent and proactive approach, by not setting expectations, this could lead to inconsistencies in practice and information security risks being introduced.

Data Sharing

- The Trust does not have sufficient oversight of data sharing activities. Without visibility or a log of data sharing activities, there is a risk of DPIAs, data sharing agreements or privacy information not being in place when required and increased risk of non-compliance with individual rights requests within the statutory timeframe.
- The Trust does not provide guidance or training to staff responsible for sharing data. When ad-hoc disclosures take place, with a lack of guidance, staff are not considering all data protection principles, individual rights and exemptions under UK GDPR and DPA 2018. This risks disclosures being disproportionate, excessive and unlawful.
- Operational staff at the Trust may get safeguarding advice without DP advice. Both safeguarding and DP laws should be considered together and exemptions under DPA 2018 applied where necessary.

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 University of Chichester (Multi) Academy Trust.

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 University of Chichester (Multi) Academy Trust. The scope areas and controls covered by the audit have been tailored to University of Chichester (Multi) Academy Trust and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.