East Surrey College

Data protection audit report

March 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.

East Surrey College (ESC) requested an audit from the ICO in November 2023 and submitted an audit questionnaire detailing the college's data protection compliance concerns. A scoping call was held with ESC to discuss the college's 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 ESC with an independent assurance of the extent to which ESC, 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 ESC's processing of personal data. The scope may take into account any data protection issues or risks which are specific to ESC, identified from ICO intelligence or ESC'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 ESC, the nature and extent of ESC's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to ESC.

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.
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.

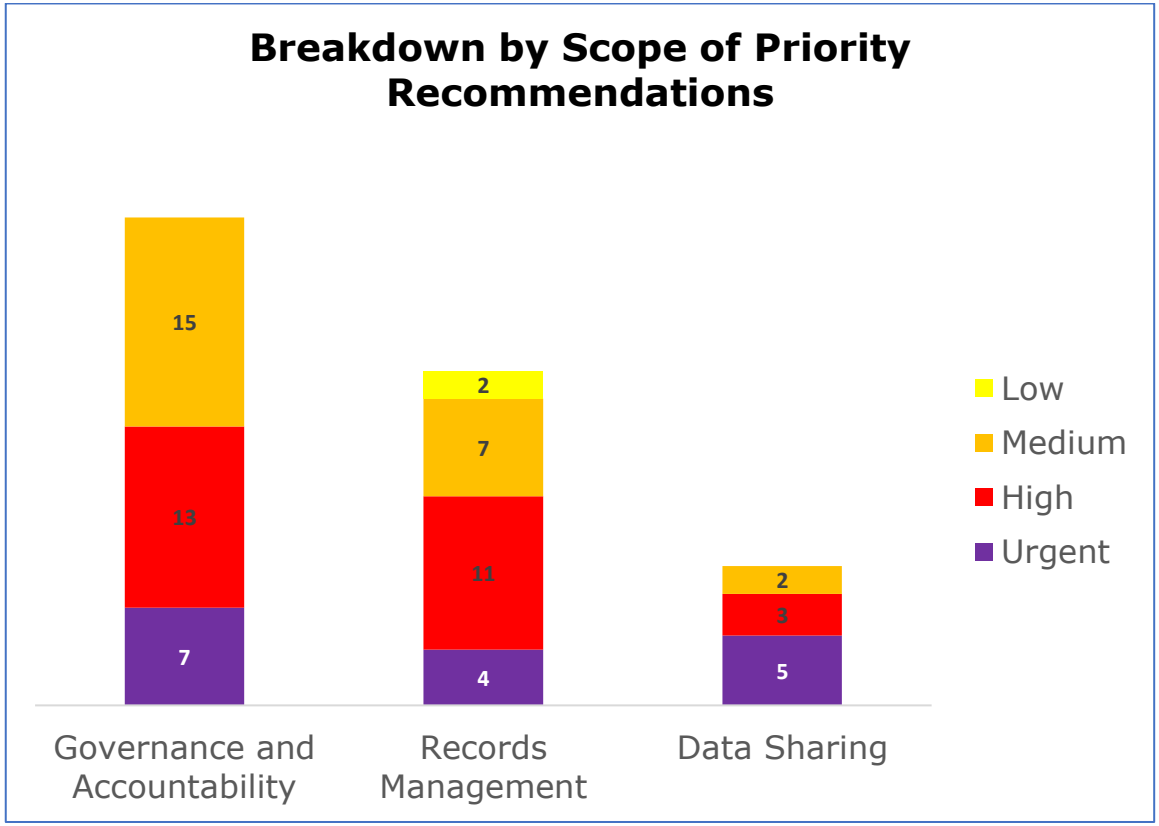
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist ESC in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. ESC'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.
Data Sharing	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 ratings above are reflective of the remote audit methodology deployed and the rating may not necessarily represent a comprehensive assessment of compliance.

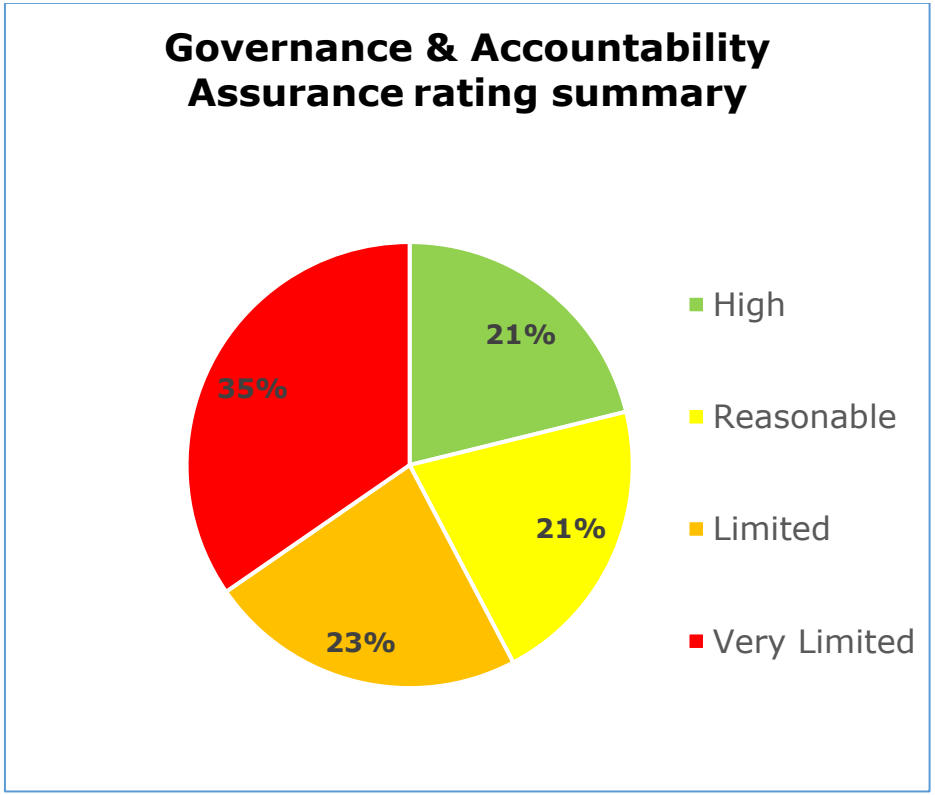
Priority Recommendations



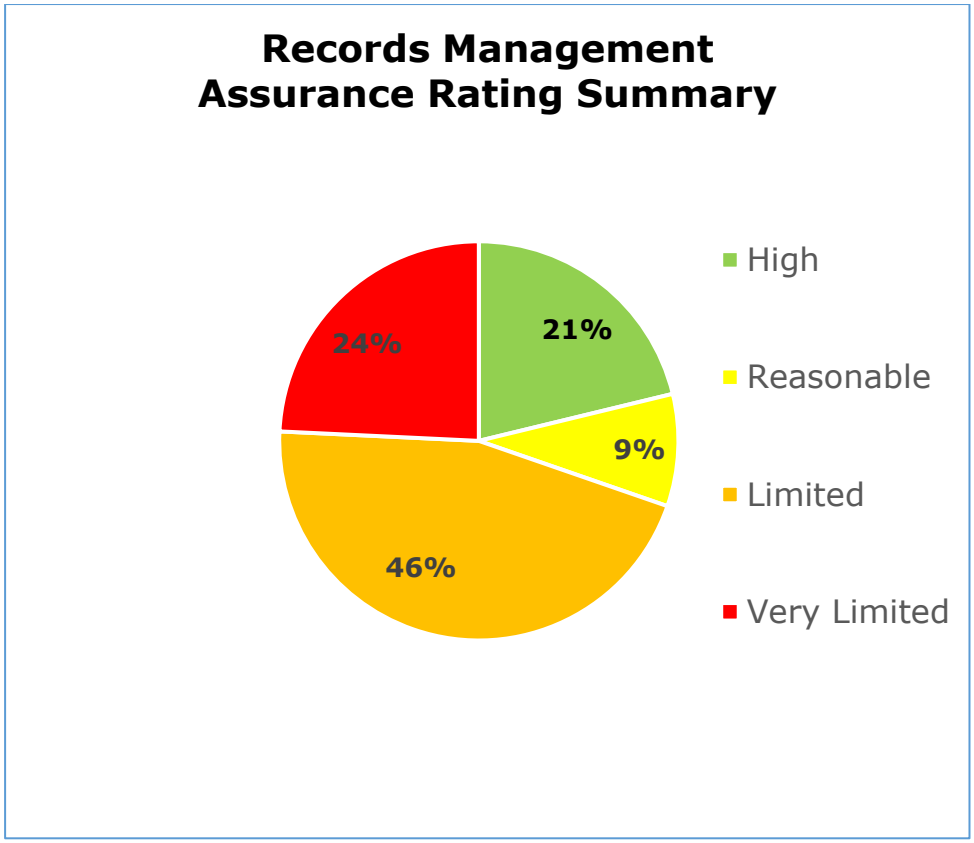
The bar chart above shows a breakdown by scope area of the priorities assigned to our recommendations made:

- Governance and Accountability has seven urgent, 13 high and 15 medium priority recommendations
- Records Management has four urgent, 11 high, seven medium and two low priority recommendations
- Data Sharing has five urgent, three high, two medium priority recommendations

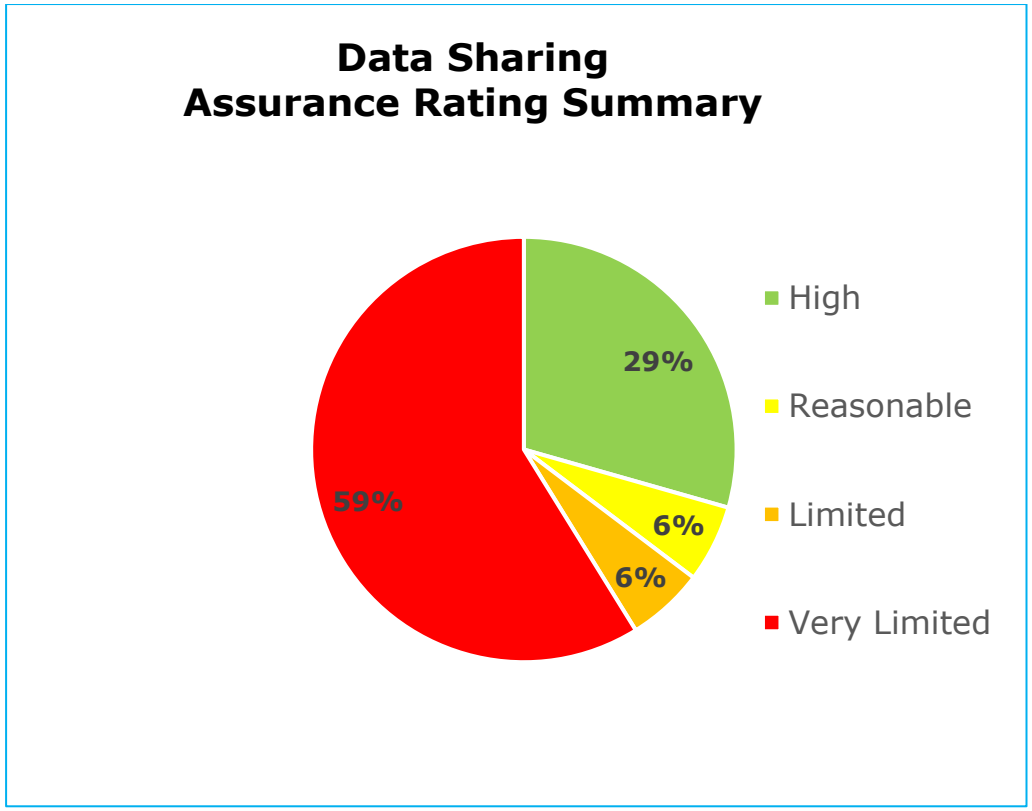
Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded in the Governance and Accountability scope. 21% high assurance, 21% reasonable assurance, 23% limited assurance, 35% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Records Management scope. 21% high assurance, 9% reasonable assurance, 46% limited assurance, 24% very limited assurance.



The pie chart above shows a summary of the assurance ratings awarded in the Data Sharing scope. 29% high assurance, 6% reasonable assurance, 12% limited assurance, 53% very limited assurance.

Areas for Improvement

Governance and Accountability

- ESC must create a privacy culture in which there is an awareness and respect for data protection, the DPO and the DPO's duties. This will enable better risk management through communication and reduce the risk of data breaches through awareness.
- ESC must complete an information audit of all departments and use the findings to create data maps and a more comprehensive ROPA. This must then be regularly reviewed and updated, ensuring that ESC is aware of all processing activities taking place.
- ESC must review their training programme and processes in order to gain assurance of staff understanding of data protection. This should include creating a training needs analysis, implementing specialist training where appropriate and effective completion monitoring.

Records Management

- ESC must establish clear responsibility for maintaining the retention schedule within job descriptions. Once these roles are embedded, ESC must conduct a review of all electronic and physical records to ensure that all personal data is deleted or destroyed in line with set retention periods.
- ESC should formally document all current processes used relating to the lifecycle of records management and circulate these procedures to all staff. This will assure ESC that all staff are meeting data protection obligations.
- ESC should use local level asset registers and the results of any information audits or data mapping exercises to create an overarching information asset register. This register should be kept under review alongside the ROPA and used to track the location of records.

- ESC must remove the use of autofill from Outlook. By encouraging staff to use the active directory or to manually add email addresses, this could reduce the number of personal data breaches. Further measures should be taken by ESC regarding the correct use of attachments, encryption and the security of personal data in transit.

Data Sharing

- ESC must review, update and create data sharing policies, procedures and registers. It is important that ESC apply the findings of ESC's information audit, the ICO Data Sharing Code of Practice and data protection legislation when developing these documents. This will help ESC create meaningful and accurate policies, procedures and records.
- ESC must document and appropriately justify its lawful basis for sharing personal data in line with UK GDPR. ESC must ensure that documentation and forms meet the requirements of the lawful basis, and that the privacy notices are updated accordingly. ESC can then ensure it is meeting its legal obligations by processing all personal data in a lawful, fair and transparent manner.
- ESC should ensure that data sharing agreements contain sufficient detail and have been implemented with data sharing partners ESC regularly share data with. This will ensure ESC are taking adequate steps to mitigates information risk.
- ESC should ensure it has agreed, documented and regularly reviews technical and organisational security arrangements around data sharing, including the transmission of the data, and procedures for dealing with any data protection breaches in a timely manner. ESC should also gain assurance that data sharing partners have sufficient security measures in place to protect the data received and transmitted. This will help ESC ensure security measures are appropriate and effective.

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 East Surrey College.

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