Rowan Learning Trust

Data protection audit report

December 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.

Rowan Learning Trust (RLT) requested an audit from the ICO in July 2022 and submitted an audit questionnaire detailing the Trust's data protection compliance concerns. ICO audit team managers completed a scoping call with RLT to further discuss the Trust's 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 RLT with an independent assurance of the extent to which RLT, 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 RLT processing of personal data. The scope may take into account any data protection issues or risks which are specific to RLT, identified from ICO intelligence or RLT'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 RLT, the nature and extent of RLT's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to RLT.
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.
Requests for Access and Data Portability	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.

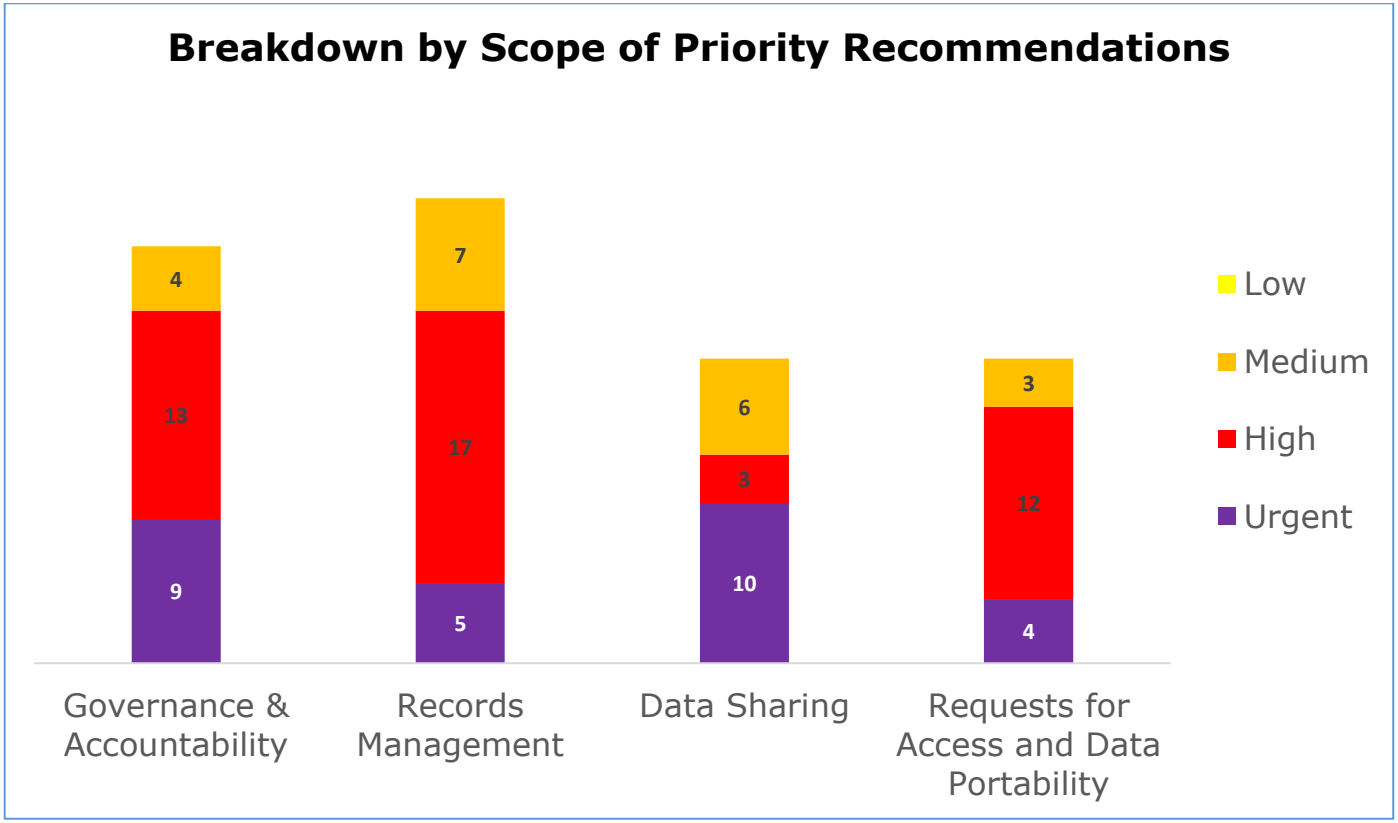
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist RLT in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. RLT'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.
Requests for Access and Data Portability	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 9 urgent, 13 high and 4 medium priority recommendations.
- Records Management has 5 urgent, 17 high, and 7 medium priority recommendations.
- Data Sharing has 10 urgent, 3 high and 6 medium priority recommendations.
- Requests for Access and Data Portability has 4 urgent, 12 high, and 3 medium priority recommendations.

Key Areas for Improvement

Governance and Accountability:

RLT currently has no oversight on its data protection management and compliance levels. Data protection compliance is currently not discussed routinely in any local groups or at Board level across the Trust, and compliance information is not reported to senior management. RLT should ensure that data protection compliance matters are standing agenda items at local and board level meetings, with compliance information being reported to senior management on a routine basis so RLT is able to demonstrate accountability and oversight of the personal information it processes.

RLT's data protection policy is not fit for purpose and does not include a supporting suite of policies and procedures to advise staff of their data protection obligations. RLT should implement a new data protection policy with supporting documentation and ensure that staff are aware of and understand the contents.

There is currently no mandatory data protection training in place for RLT staff. RLT should implement a mandatory data protection training programme which covers induction and annual refresher training, and specialised training for staff in information governance roles.

RLT does not have a Record of Processing Activity (ROPA) document in place. RLT should create its ROPA document as soon as possible so it can demonstrate it has adequately recorded essential information regarding all of its personal data processing activities, as required by Article 30 of the UK GDPR.

Records Management:

There is currently no oversight of Records Management (RM) or operational responsibility assigned to a Records Manager. RLT have recently appointed a Senior Information Risk Owner (SIRO) who will have lead responsibility for the oversight of RM. They should also assign operational responsibility for the RM function to a Records Manager. This will ensure that RLT has oversight and direction in place at a senior level for its RM function.

RLT have not conducted an information audit, so do not have an understanding of all of the information that is held and how it flows across the Trust. RLT have acknowledged that an information audit needs to be completed. This will ensure that they are aware of what information it holds, how it is processed, and where that processing takes place within the Trust.

There are currently no compliance checks carried out across RLT to ensure that physical and electronic records are destroyed in line with their retention periods. RLT should have processes in place to ensure physical and electronic records are deleted according to the retention schedule. They must also assign appropriate responsibility to designated staff for retention and disposal across RLT.

RLT do not have contracts in place with the confidential waste disposal companies they use. They must create contracts for them and complete occasional checks, to ensure they are fulfilling their contractual agreements and appropriately disposing personal data.

Data Sharing:

RLT do not currently conduct data protection impact assessments (DPIAs) or maintain a DPIA log. By introducing DPIAs RLT will be able to demonstrate that it has assessed the risks related to sharing personal data and manage these risks appropriately.

RLT do not have a data sharing agreement (DSA) template or log. RLT should ensure that these documents are created so DSAs are managed consistently across the Trust, and are compliant with the Data Sharing Code.

RLT does not have sufficient security measures in place around the sharing of personal data. RLT should ensure it comprehensively assesses, and periodically reviews the security measures of the organisations it shares data with.

RLT should ensure it has adequate policies and procedures for managing ad hoc third-party, emergency, and critical situation requests, so that they are handled appropriately to reduce the risk of a personal data breach or a breach of the legislation.

Requests for Access and Data Portability:

External facing policies were found to be inconsistent across RLT and its schools. It was also determined that the Trust has not made these policies available to suit different audiences. The Trust should review all external policies to ensure consistency across all schools and make these policies available in different languages. The Trust should also test their pupil privacy policies on children of different ages to check for adequacy.

RLT staff should also be made aware of any changes made to external policies to effectively communicate them to any requestors.

There is no awareness within the Trust on the procedure for conducting identity checks or for the appropriate disclosure of personal data of mature children. RLT should ensure the guidance on completing identity checks within the data protection policy is communicated to staff and require staff to read it. If RLT creates a separate

SAR policy, this information should be included. The practice of completing identity checks, either through the SIMs system or requesting further proof should be enforced. Staff should be given training on testing for competency in children over the age of 12. Reference to these checks should be reflected in both internal and external policies to ensure staff, parents and pupils are made aware of what can be requested, by who and when consent will need to be gained.

Staff are unaware of the statutory deadlines for completing SARs including school holidays, extensions and when to 'stop the clock'. RLT should make any staff who are responsible for SARs aware of the statutory deadlines regarding school holidays as soon as possible and assign an adequate number of staff who work throughout holidays the responsibility for SARs to ensure each request is acknowledged and processed without delay.

RLT should update both their internal and external policies to provide accurate written guidance for transparency.

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