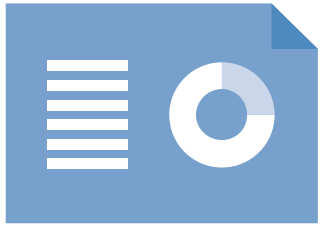
Ormiston Academies Trust

Data protection audit report

August 2019

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (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 sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Ormiston Academies Trust (OAT) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 10 May 2019 with representatives of OAT to discuss the scope of the audit.

Telephone interviews were conducted on 24 June 2019, 26 June 2019 and 28 June 2019 prior to the onsite visit. The audit fieldwork was undertaken at OAT's Offices, Birmingham, and Ormiston Forge Academy Cradley Heath, on 3 July 2019 and 4 July 2019.

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

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

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 GDPR and national data protection legislation are in place and in operation throughout the organisation.
Training & Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

The audit was 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, on-site visits including interviews with selected staff, and an inspection of selected records.

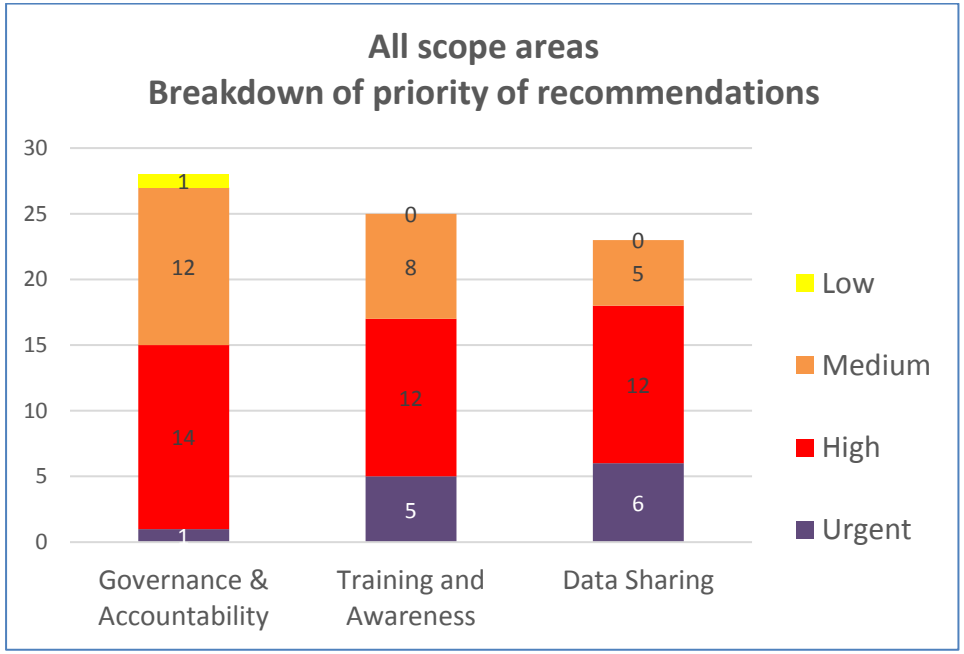
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist OAT in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. OAT'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	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Training & Awareness	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.

ICO Assurance Ratings
High
Reasonable
Limited
Very Limited

Priority Recommendations



Recommendation Priority Ratings Descriptions
Urgent Priority Recommendations - 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 - 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 - 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 – 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.

Good Practice

ICO auditors acknowledge that OAT have been working positively towards GDPR compliance, and in particular the installation and training of data protection leads at each academy is a positive step. This means that OAT already have in a place a structure that will enable the improvements recommended in this report to be implemented effectively across all of OAT's 38 academies.

Areas for Improvement

Put in place a formalised DPIA procedure, i.e. a prescribed risk assessment for high risk processing which assesses the impact on the rights and freedoms of the data subjects and sets out the subsequent mitigations to control these risks.

Update all existing contracts with data processors so that they fully comply with Article 28 of the GDPR.

Nominate one of OAT's trustees to be the individual with responsibility for Information Governance and Data Protection to help ensure compliance with Article 5 (2) of the GDPR; the accountability principle.

Put in place a system to ensure there is specific role based training provided to key members of staff with information governance and data protection responsibilities.

Ensure that training completion rates are monitored at head office and academy level.

Ensure that there is oversight of additional or specialised training used by the academies. It is important that there is mandated criteria for the third party providers such as an assessment or minimum pass rate.

Put in place a system of formalised assessment of the legality of data sharing. This should include a determination of whether there is a lawful basis for sharing, an express or implied legal power; and in the case of special category data that the necessary condition for processing in the GDPR and Data Protection Act 2018 can also be satisfied.

Ensure there are data sharing agreements in place in relation to controller to controller data sharing arrangements and that they include high level matters such as setting out the common rules to be followed by all partners. They should also include, for example, formalised arrangements for the reporting, investigation and resolution of security incidents.

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