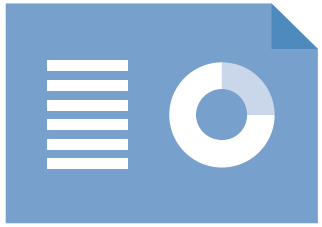
Academies Enterprise Trust

Data protection audit report

May 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.

Academies Enterprise Trust (AET) agreed to a consensual audit by the ICO of its processing of personal data. An introductory meeting was held on 17 December 2018 with representatives of DAT to discuss the scope of the audit.

Telephone interviews were conducted on 6 March 2019 and 7 March 2019 prior to the onsite visit. The audit fieldwork was undertaken at AET Offices, London, and Aylward Academy, London, between 12 March 2019 and 13 March 2019.

The purpose of the audit is to provide the Information Commissioner and AET with an independent assurance of the extent to which AET, 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.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.
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.

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 AET 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

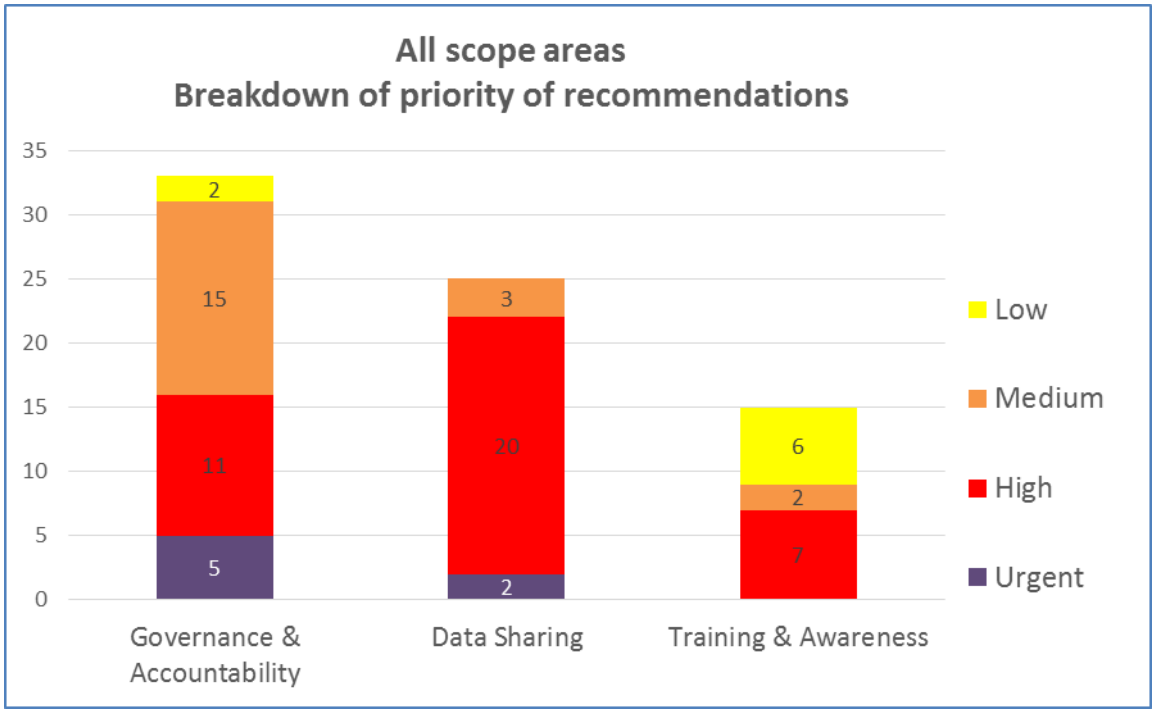
the ICO's assessment of the risks involved. AET's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

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.
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.

Training & Awareness	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.

Priority Recommendations



Areas for Improvement

AET should complete an information flow mapping exercise and use the results to produce records of processing activities as required in Article 30 of the GDPR.

The risk management process within AET should be developed to include granular risks of non-compliance with data protection legislation to improve the identification, management and mitigation of current and future risks.

Improve the system that ensures data processors are complying with all of their obligations under data protection legislation so that AET have assurance their personal data is processed in line with the GDPR.

AET should expand their programme of internal based audit and compliance checks to ensure data protection legislation and internal policies and procedures are being complied with.

AET should review existing data sharing agreements to ensure they are up to date and meet the requirements of the GDPR. All agreements should be recorded on a central log to improve AET's oversight and management of the personal data they share.

The data protection training programme at AET should be expanded to include records management and information security along with sector specific content to increase staff awareness.

Good Practice

ICO auditors acknowledge that AET are working positively towards GDPR compliance. It was noted that there was a programme of data protection awareness for staff in place, including the #OneAET portal which collates relevant data protection information and policies for staff in one place.