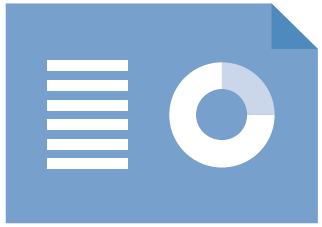
Delta Academies Trust

Data protection audit report

March 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.

Delta Academies Trust (DAT) agreed to a consensual audit by the ICO of its processing of personal data. An introductory meeting was held on 12 November 2018 with representatives of DAT to discuss the scope of the audit.

Telephone interviews were conducted on 31 January 2019 and 1 February 2019 prior to the onsite visit. The audit fieldwork was undertaken at DAT Offices, Knottingley, and De Lacy Academy, Knottingley, between 5 February 2019 and 6 February 2019.

The purpose of the audit is to provide the Information Commissioner and DAT with an independent assurance of the extent to which DAT, 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.

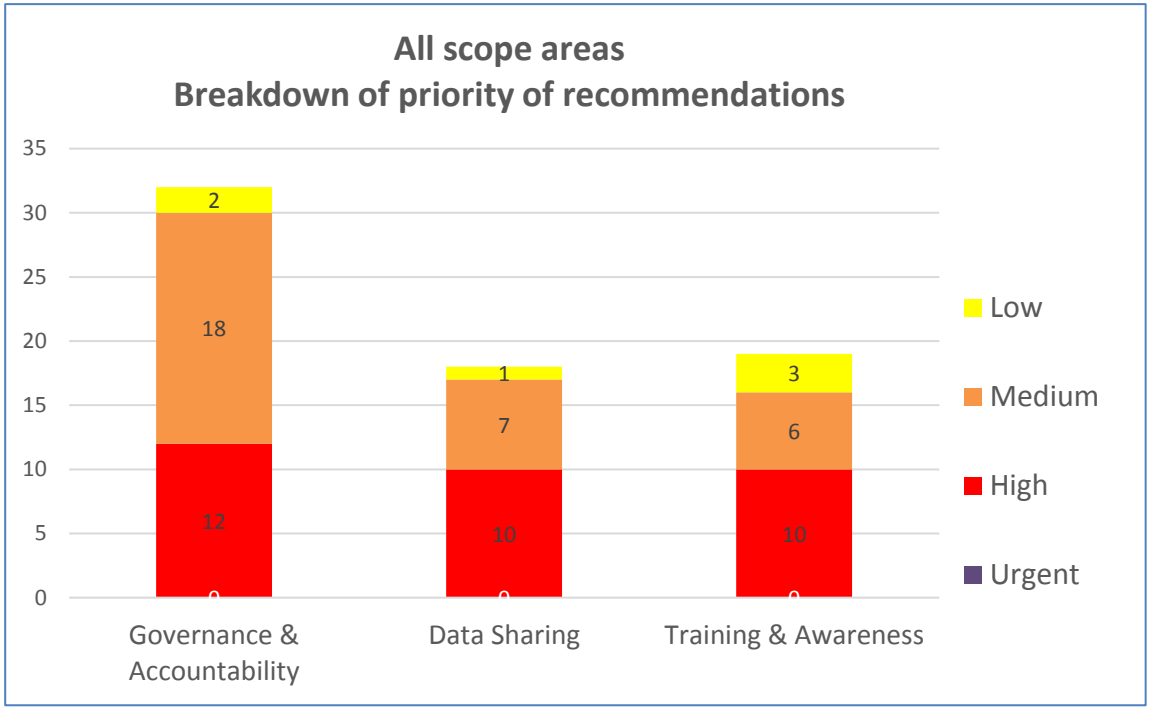
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist DAT 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. DAT's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

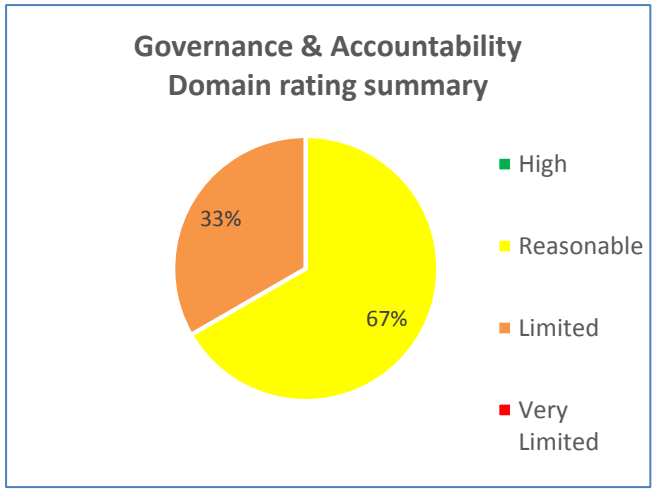
Audit Summary

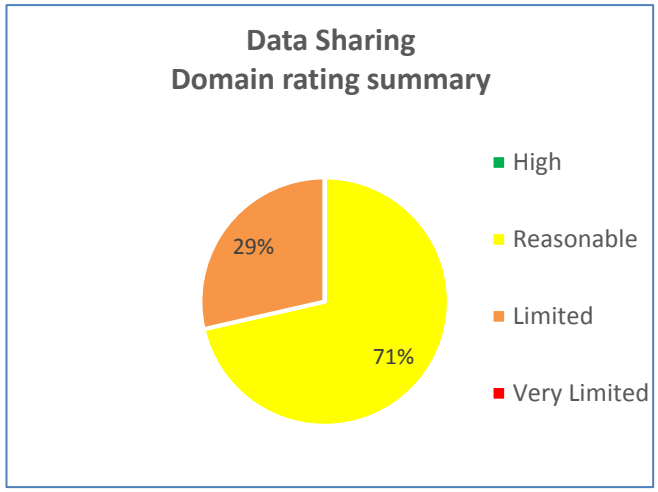
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	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.

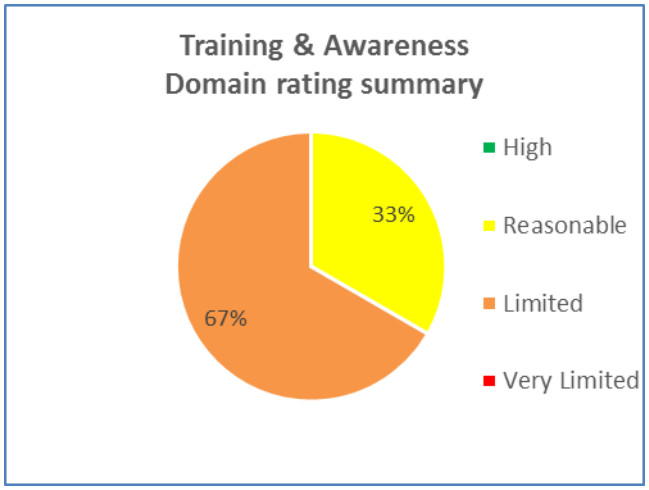
Priority Recommendations



Graphs and Charts







Areas for Improvement

DAT should continue with plans to recruit a new Board member as soon as possible, with the skills and expertise to become the member with responsibility for data protection/information governance.

DAT should break down the risk of non-compliance with data protection legislation at a more granular level, and could choose to document this on their corporate risk register or develop a dedicated Information Risk Register.

A log of sharing agreements should be kept centrally which details the nature of the sharing and the partners. This should include, for example, the data being shared - its volume, type, sensitivity and classification, who the data is being shared with including key points of contact, the methods of transmission for the data, when each DSA should be reviewed and the date of the last review, retention or deletion dates for the data shared and when the last audit was conducted to confirm compliance to agreement requirements.

A Training Needs Analysis (TNA) exercise should be carried out across all staff roles at DAT, including temporary and contract staff with access to personal data.

DAT should ensure that as part of any training programme, refresher training is completed at least annually by all staff.

Good Practice

ICO auditors acknowledge that DAT have been working positively towards GDPR compliance. It was noted that there was a programme of data protection awareness for staff in place, with posters up onsite.

An onsite compliance check has been conducted to test security arrangements at one data processor.

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