

Outwood Grange Academy Trust

Data protection audit report

September 2019

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.

Outwood Grange Academies Trust (OGAT) has agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 1 July 2019 with representatives of OGAT to discuss the scope of the audit.

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

It was agreed that the audit would focus on the following areas:

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.

A review of OGATs policies, procedures and other key documents was carried out in September 2019 prior to the onsite visit. Telephone interviews were conducted on 17 September 2019 and 18 September 2019. The audit on site visit was undertaken at OGAT's head office, Potovens Lane, Outwood, Wakefield WF1 2PF from 24 September 2019 to 26 September 2019.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist OGAT 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

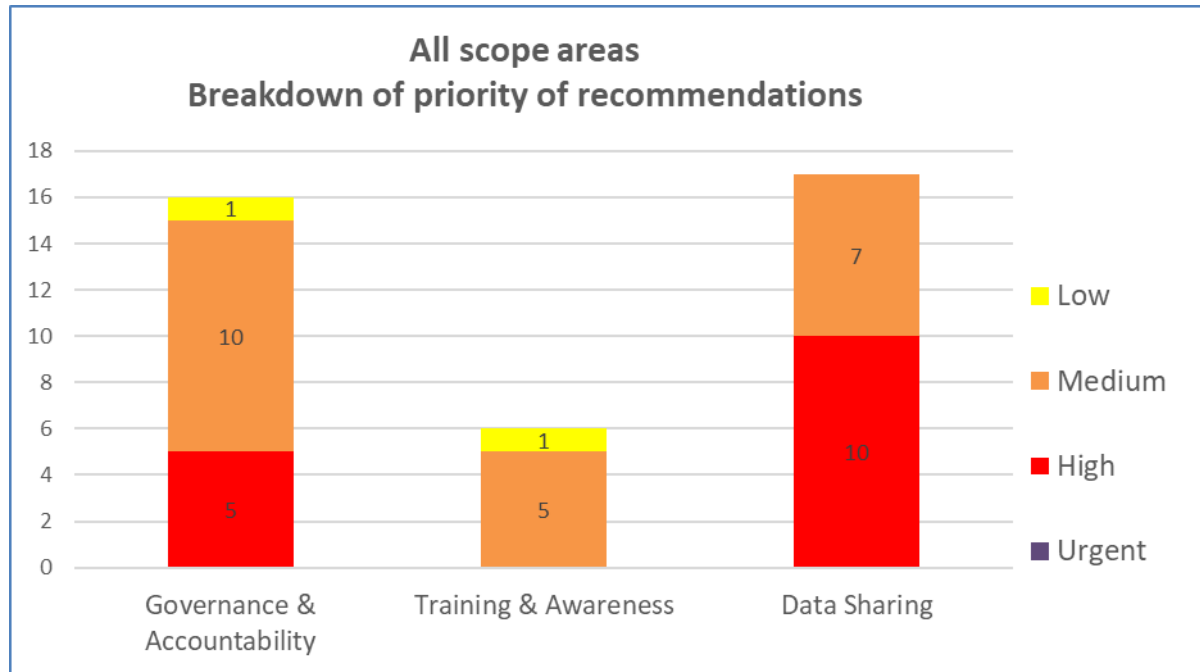
the ICO's assessment of the risks involved. OGAT priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

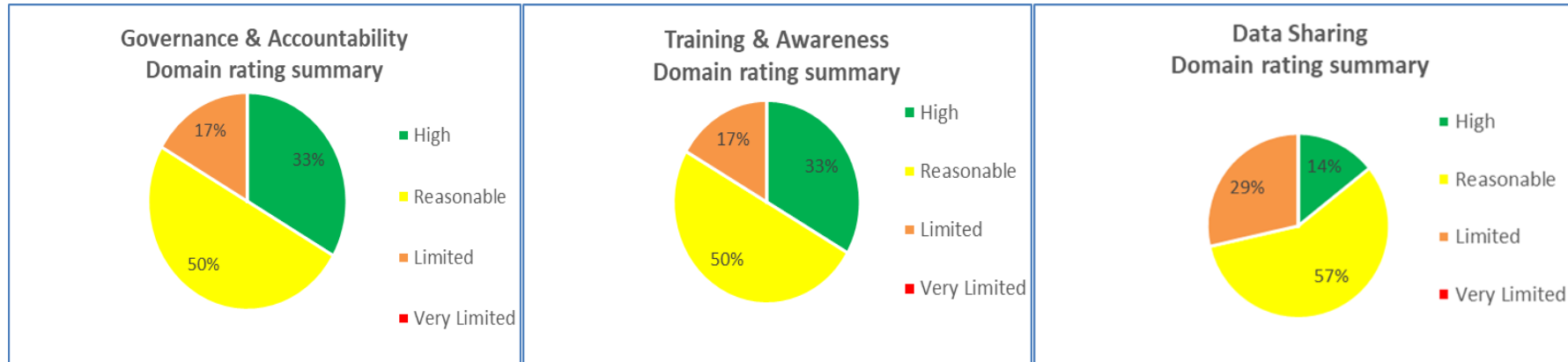
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Training & Awareness	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.

ICO Assurance Ratings
High
Reasonable
Limited
Very Limited

Charts



Charts



Good Practice

ICO auditors acknowledge that OGAT have been working positively towards GDPR compliance, and in particular senior management accountability, reporting structures across the academy and the roll out of Data Protection training are positive steps. This means that OGAT already have in place a structure that will enable the improvements recommended in this report to be implemented effectively across all OGAT's academies.

Areas for Improvement

Data protection training should include more detailed specialised course content around records management and data sharing to help reduce the risk of non-compliance with GDPR Article 5 (c), (d) and (e);

To help meet the requirements of GDPR Article 5, OGAT should implement key performance indicators around records management and information governance

OGAT should develop a needs based training program to regularly assess all staff groups;

OGAT should develop procedures to help staff identify any exemptions that may apply from the DPA18 Schedules 3 and 4 when they receive requests for personal data disclosure;

OGAT should implement a quality assurance process for adhoc third party data sharing requests;

OGAT should develop a policy that will address how records are used within the trust; and

As part of OGAT's obligations under GDPR Article 28, more robust compliance checks on processors should be implemented to ensure the effectiveness of data handling and security controls.

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