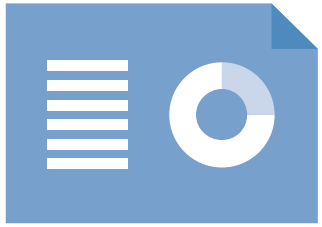
Active Learning Trust

Data protection audit report

January 2019

ico.
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.

The Active Learning Trust (ALT) agreed to a consensual audit by the ICO of its processing of personal data. An introductory meeting was held 10 May 2018 with representatives of ALT to discuss the scope of the audit.

Telephone interviews were conducted on 11 October 2018 and 15 October 2018 prior to the onsite visit. The audit fieldwork was undertaken at ALT's Office, Ely and Neale Wade Academy, March between 16 October 2018 and 18 October 2018.

The purpose of the audit is to provide the Information Commissioner and ALT with an independent assurance of the extent to which ALT 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.
Requests for personal data & data portability	There are appropriate procedures in operation for recognising and responding to individuals' requests for access to or to transfer their personal data.
Data Sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

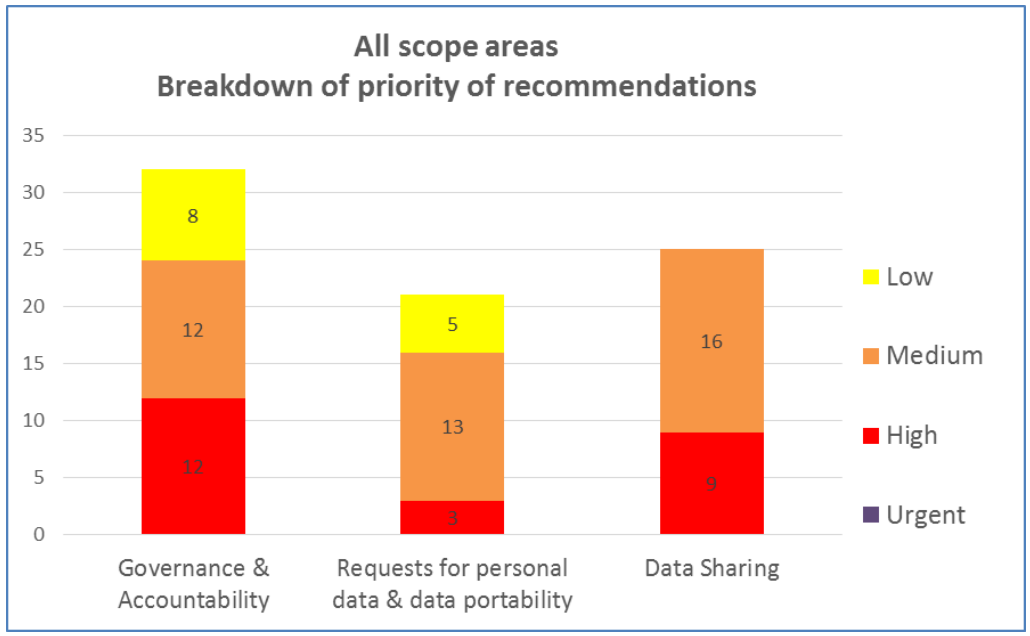
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

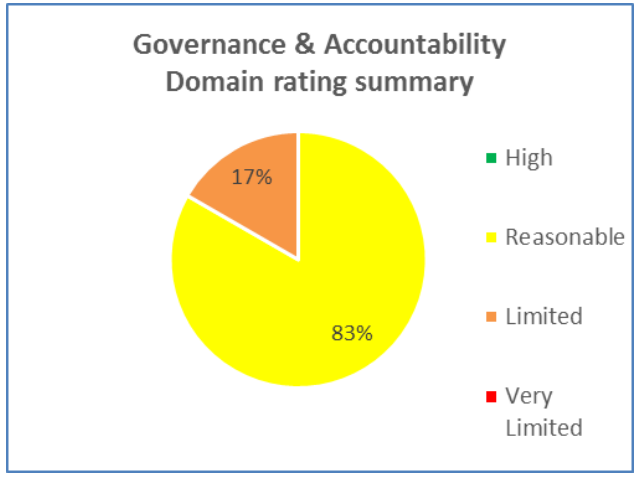
Audit Summary

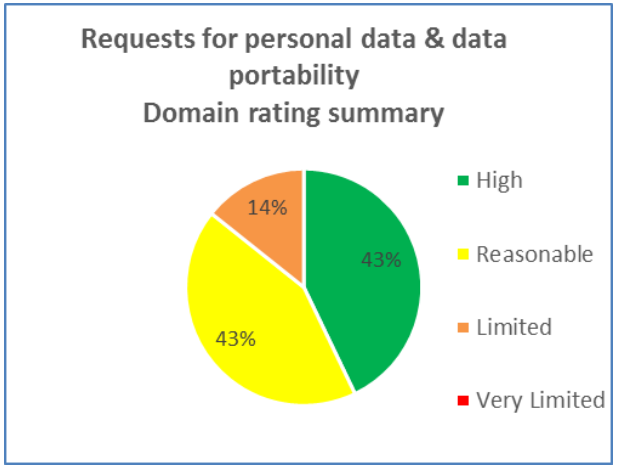
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce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

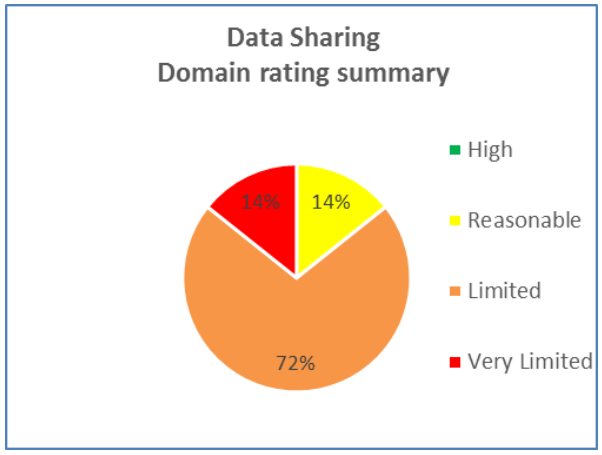
Priority Recommendations



Graphs and Charts







Good Practice

It is acknowledged that ALT have focused key resources and taken considerable steps over the last six months to address GDPR compliance. ALT have introduced a number of measures, such as a suite of Information Governance Policies, a GDPR Toolkit, data protection newsletters as well as ICT security audits and IT standards which have made a positive impact on their GDPR compliance. In addition, there is a comprehensive policy and procedure for subject access requests as well as a model letter pack.

Areas for Improvement

ALT should document fully its risk management process, including how risks are escalated.

A programme of regular internal data protection audits should be implemented. Routine compliance checks should be recorded and reported on.

ALT should introduce annual, mandatory information governance training for all staff and report on this as a key performance indicator. Training should include how staff should recognise a subject access request.

Specialist training for key staff in areas such as subject access requests, data sharing, and data protection impact assessments should be introduced.

ALT should document fully its approach to data sharing and record the details of all data sharing and data sharing decisions centrally.

A process for dealing with ad hoc disclosures should be formulated and embedded.

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