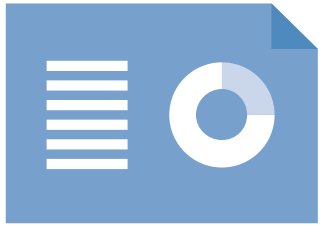
Northern Education Trust

Data Protection Audit Report – Executive Summary

October 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.

Northern Education Trust (NET) 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 NET to discuss the scope of the audit.

Telephone interviews were conducted on prior to the onsite visit. The audit fieldwork was undertaken at NET's offices at North Shore Academy, Stockton-On-Tees on 17 – 19 September 2019.

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

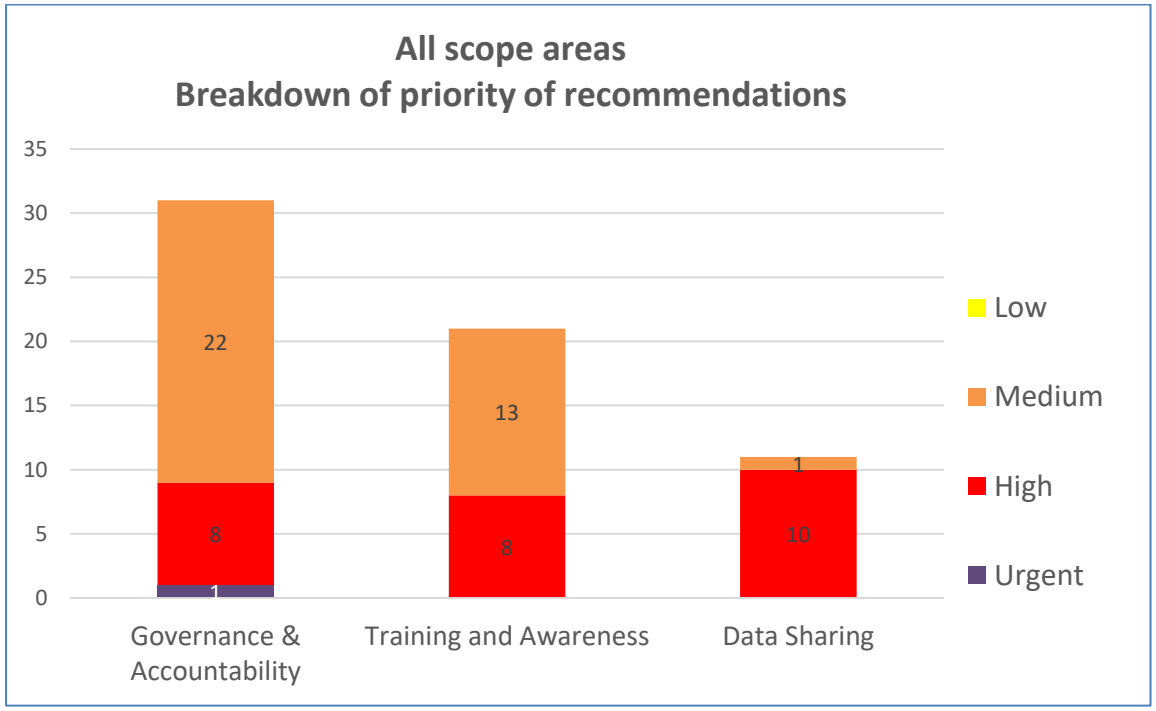
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

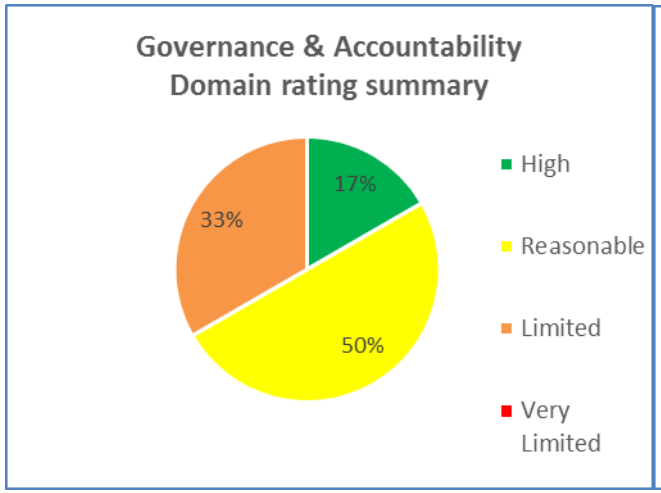
Priority Recommendations

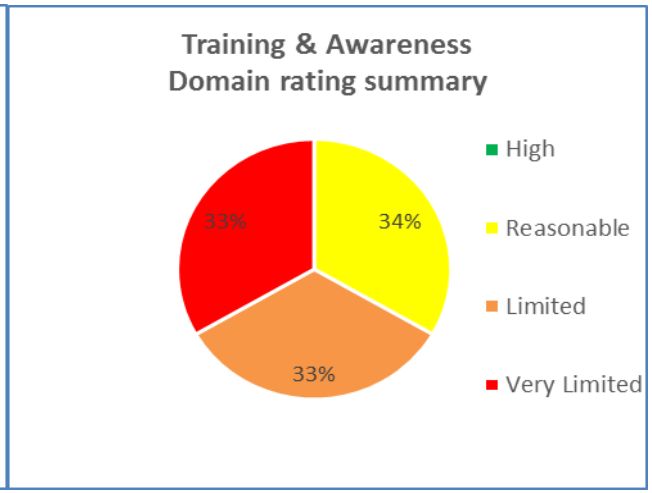


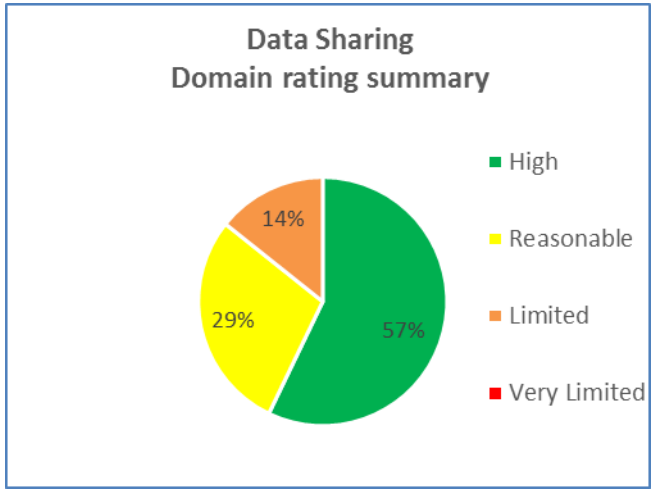
Recommendation Priority Ratings Descriptions:

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.

Graphs and Charts







Areas for Improvement

Governance and Accountability

Improved oversight of actions agreed by the Information Governance Steering Group (IGSG) should be provided by the creation of an Action Plan to record and evidence the ownership, progress and outcomes of these actions.

Business Managers' job descriptions should be aligned to their responsibilities for Information Governance (IG).

Information Asset Owners (IAOs) should be assigned to NET's systems and assets and recorded appropriately on its Information Asset Registers (IARs)

Training and Awareness

The IGSG should complete its review of data protection training to ensure that specific roles receive appropriate specialised training in this area.

There should be a formalised follow up process for non-attendees at mandatory data protection training, and NET should also consider setting personal development objectives which relate to this training.

Data Sharing

Means to provide assurance of full oversight of data sharing within the Trust should be investigated and implemented.

Work should continue to ensure that Data Sharing Agreements (DSAs) are in place where required. These should all be signed off by senior management in each organisation, and logged centrally with a review process in place.

Good Practice

NET have introduced a rolling programme of site visits in order to gain formalised assurances that Information Security processors are demonstrating good practice in data protection.

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 NET.

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