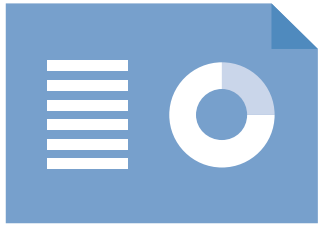
North Norfolk Academy Trust

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.

North Norfolk Academy Trust (NNAT) agreed to a consensual audit by the ICO of its processing of personal data. An introductory meeting was held 21 September 2018 with representatives of NNAT to discuss the scope of the audit.

Telephone interviews were conducted on 14 December 2018, 17 December 2018 and 10 January 2019 prior to the onsite visit. The audit fieldwork was undertaken in the County of Norfolk at Stalham High School, Sheringham High School, Gresham Village School and Antigham and Southrepps Primary School between 15 January 2019 and 16 January 2019.

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

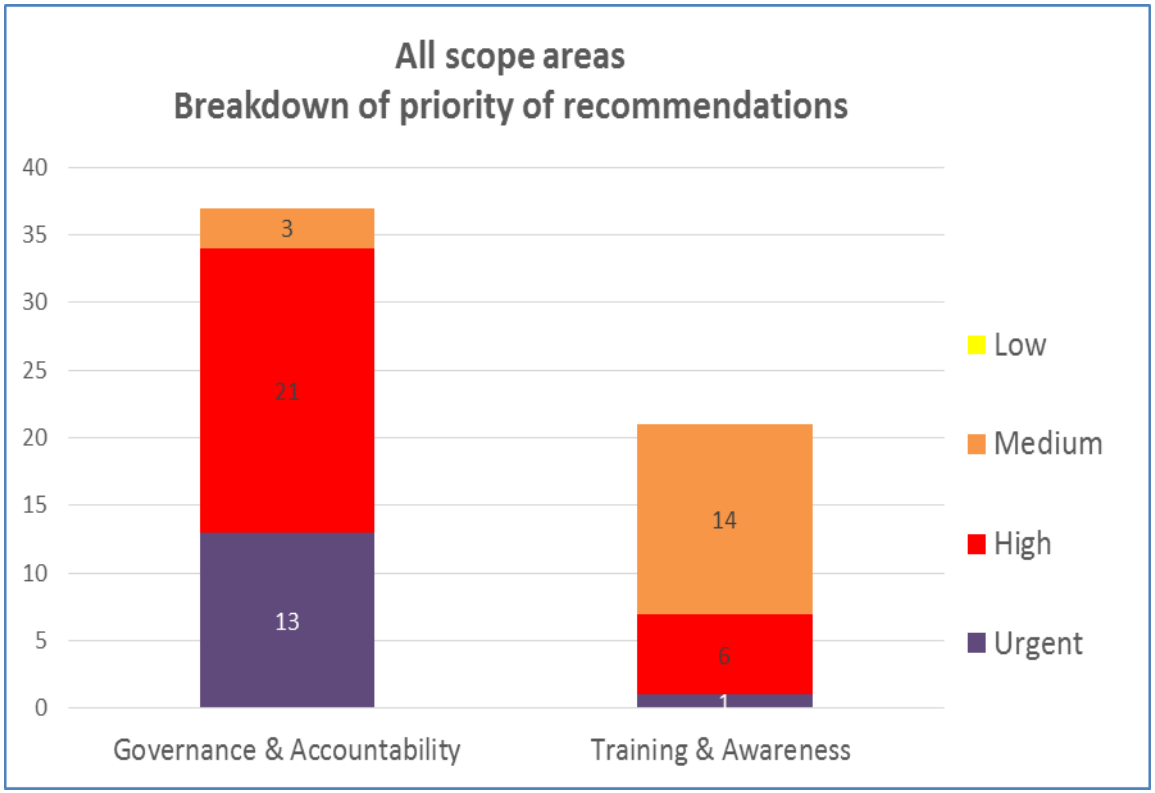
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

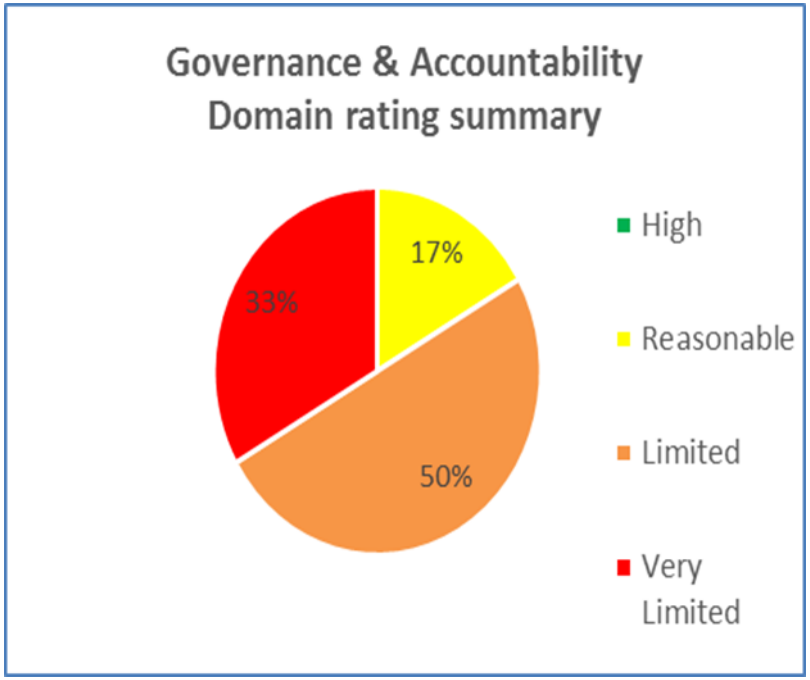
Audit Summary

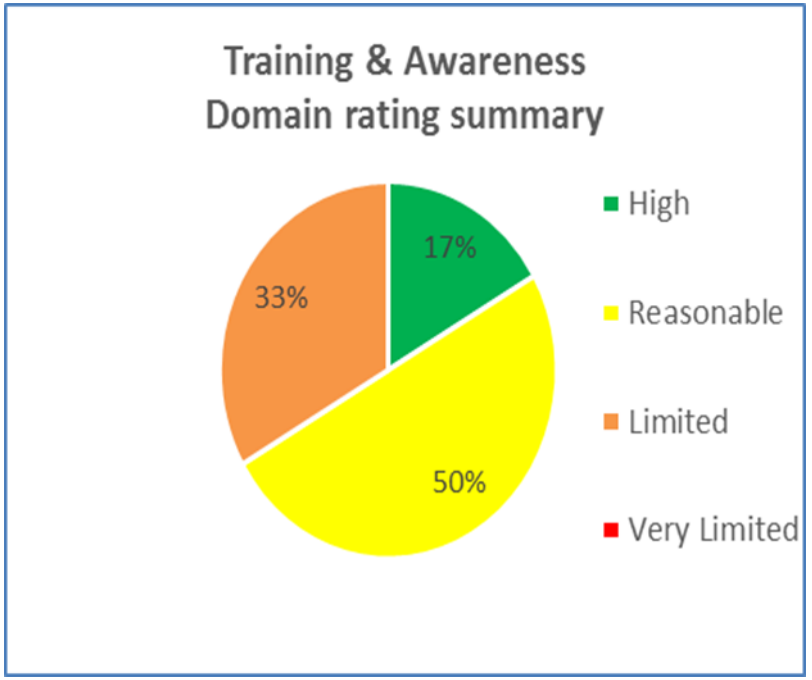
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to 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



Graphs and Charts





Good Practice

ICO auditors acknowledge that NNAT have been working positively towards GDPR compliance. There was a good level of data protection awareness amongst staff promoted via a series of posters, emails and by the Data Protection Officer (DPO) role.

Areas for Improvement

A system of Key Performance Indicators (KPIs) should be introduced to ensure that senior management of the trust are able to monitor key areas of compliance with data protection (DP) legislation. Key areas include; records management (RM), information security (IS), information requests and information governance (IG) training.

A risk based internal audit function should be implemented, together with routine compliance checks.

NNAT should create central and academy level action plans to provide structure to NNAT's continuing and improving compliance with DP legislation, and ensuring there is consistent practice in each of the four academies.

A Training Needs Analysis (TNA) and training plan should be formally documented to outline NNAT's approach to DP training for staff at all levels. This should also include reference to any specialist training required by key staff. These documents should be reviewed annually and approved by the Board of Trustees.

NNAT should either seek assurances from employment agencies that temporary, contract and supply staff have received a sufficient level of DP training for their role or consider providing training themselves.

IG training completion statistics should be reported on frequently to the Board of Trustees and/or Senior Management Team (SMT).

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