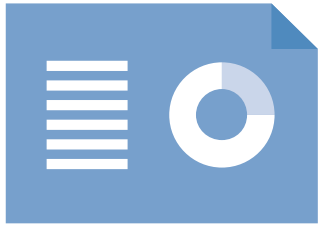
Focus Trust

Data protection audit report

October 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.

Focus Trust is a Multi-Academy Trust (MAT) comprising of fifteen primary academies across the North of England. Circa 7,000 pupils are enrolled across the academy network and 900 staff members, including agency and supply staff members, are employed, who are supported by volunteers at academy-level.

Focus Trust agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 25 July 2019 with representatives of Focus Trust to discuss the scope of the audit.

The audit fieldwork was undertaken at Focus Trust's Central Office, Oldham and Coppice and Roundthorn Primary Academies, Oldham on 22 October 2019 and 23 October 2019.

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

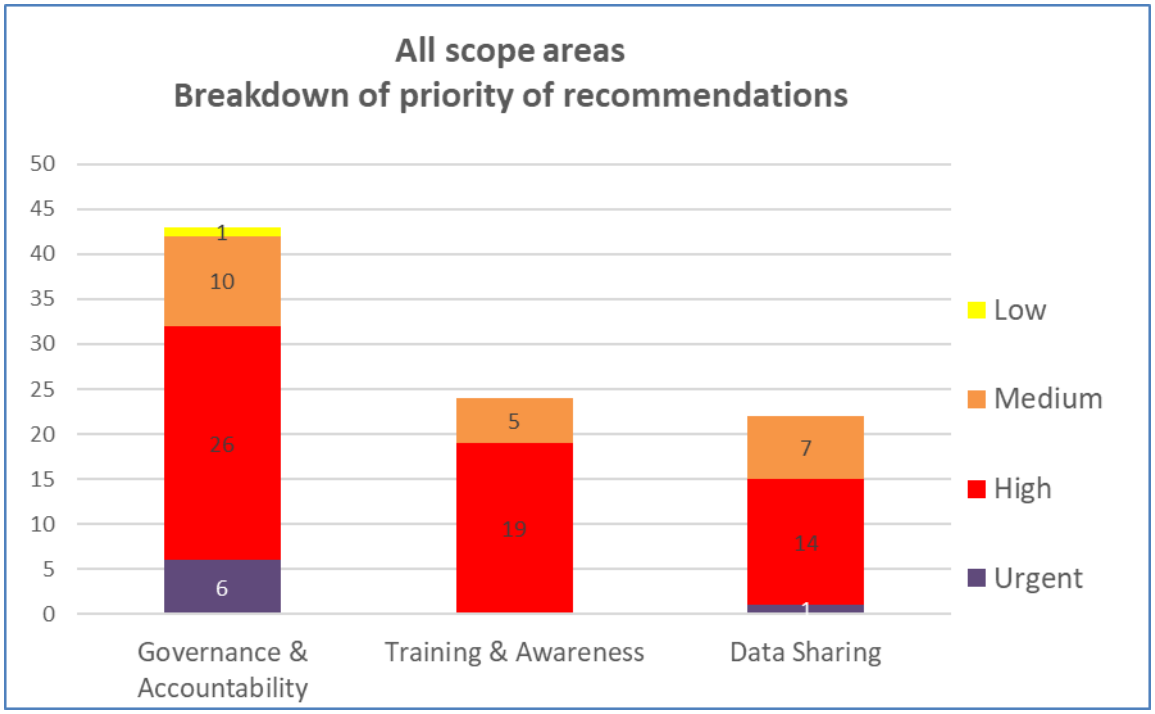
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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

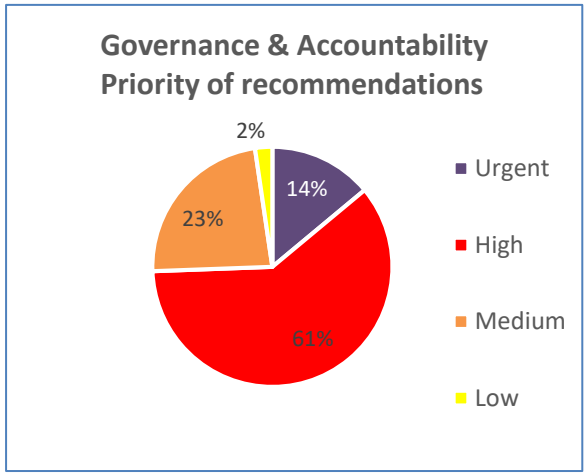
Audit Summary

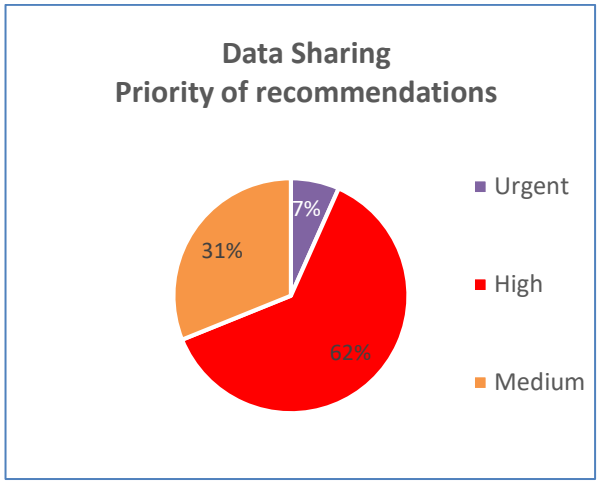
Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to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

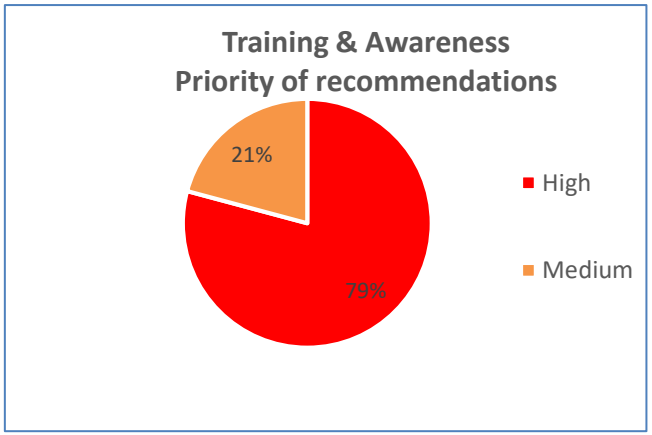
Priority Recommendations



Graphs and Charts







Areas for Improvement

A Record of Processing Activities (ROPA) should be put in place, as required by Article 30 of the GDPR. The data mapping exercise should be used to initiate this process and the ROPA should be regularly reviewed.

An Article 6 lawful basis for processing activities should be identified in relation to personal data. Where special category data has been identified, an Article 9 condition should be also be identified and recorded.

The Trust should review all privacy information and explain the Article 6 lawful basis (es) relied on, as required by Article 13 of the GDPR. Additionally, an Article 9 condition should be explained where special category data is processed.

Role and function specific training needs should be documented in a Training Needs Analysis (TNA) and a programme of training be provided accordingly. In particular, ensuring that more specific data protection training is provided, such as, for the data protection officer (DPO), the senior risk owner and data sharing roles.

A Data Protection Impact Assessment (DPIA) process should be put in place, whereby the implementing of any new systems is screened for privacy considerations prior to being used and DPIAs carried out for high risk processing.

Designate responsibility for the security of personal data at a senior level and introduce a programme of information security audits to ensure that the data held is secure.

Focus Trust should define and document how risks are managed in an appropriate policy document. This should include the approach to the identification and escalation of risk from academy level through to the Trust Board.

Put in place formalised Data Sharing Agreements to govern the practices and arrangements where personal data is routinely shared with other data controllers.

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