

United Learning Trust

Data protection audit report

April 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.

United Learning Trust (ULT) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 6 December 2018 with representatives of ULT to discuss the scope of the audit.

Telephone interviews were conducted on 27 February 2019, 28 February 2019 and 1 March 2019 prior to the onsite visit. The audit fieldwork was undertaken at ULT Offices, Peterborough, and Kettering Buccleuch Academy (KBA), Kettering, on 5 March 2019 and 6 March 2019.

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

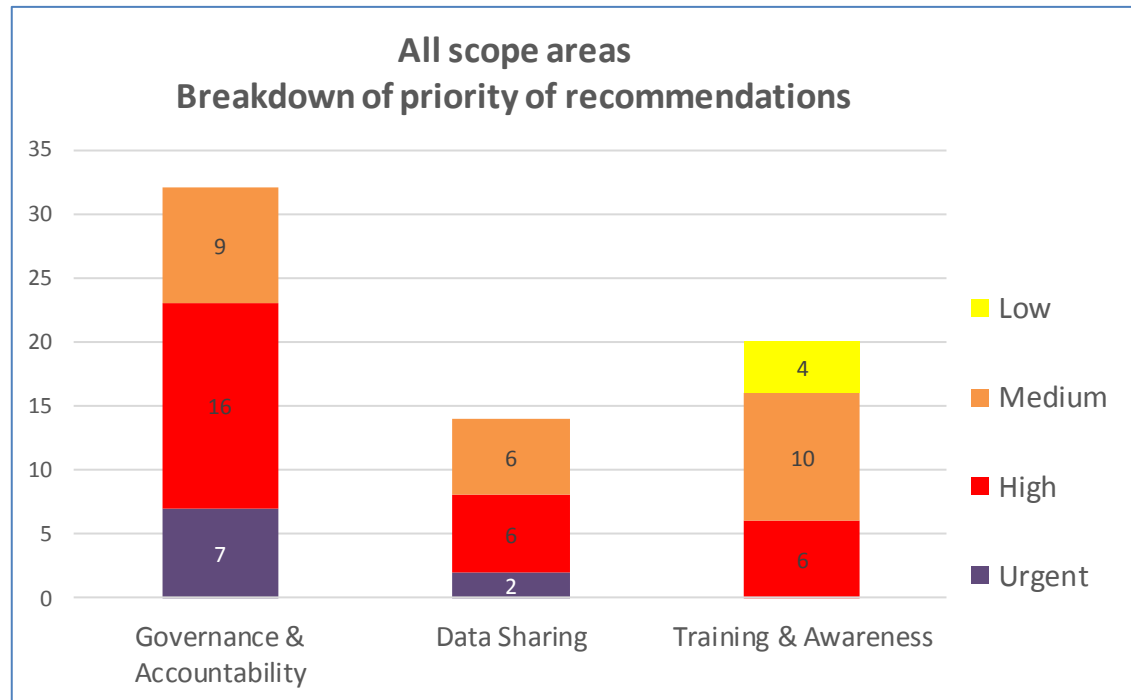
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

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



Good Practice

ICO auditors acknowledge that ULT have been working positively towards GDPR compliance, and in particular the installation and training of data protection leads at each academy is a positive step.

Areas for Improvement

- Nomination of individual at Group Board level to provide ultimate accountability for Information Governance (IG) and Data Protection legislation compliance. This person should have the skills and expertise to enable them to have overall responsibility for Data Protection and Information Governance at ULT.
- Provide a greater level of oversight of ULT Data Protection leads at academies to ensure closer control of academy level compliance, for example with regard to production and publication of privacy notices.
- Make improvements to the system that ensures data processors are complying with all of their obligations under data protection legislation.
- Ensure that data sharing agreements governing the procedures for the systematic sharing of personal data from controller to controller are put in place for all existing arrangements. If an individual controller refuses to enter into a data sharing agreement, their decision to do so should be evidenced and documented on a central system.
- Any one off collections of data (e.g. for surveys) should be supported by granular privacy statements, stating specifically how the data will be used at each point.
- Devise and roll out annual GDPR refresher training.
- Continue with plans to roll out the new Information Security (IS) training video, which should be in place as soon as possible.

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