APPENDIX A

Leicestershire County Council

Data protection audit report

Executive summary
November 2017

Information Commissioner's Office

1. Background

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51(7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

Leicestershire County Council (LCC) agreed during December 2016 to a consensual audit by the ICO of their processing of personal data.

An introductory meeting was held on 12 July 2017 with representatives of LCC to identify and discuss the scope of the audit and after that on 2 August 2017 to agree the schedule of interviews.

The audit field work was undertaken at County Hall during 12-13 September 2017.

2. Scope of the audit

Following pre-audit discussions with LCC, it was agreed that the audit would focus on the following areas:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

c. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

3. Audit Approach

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, onsite visits including interviews with selected staff, and an inspection of selected records.

The purpose of the audit was to provide the Information Commissioner and LCC with an independent assurance of the extent to which LCC, within the scope of this agreed audit, is complying with the DPA.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA.

In order to assist data controllers in implementing the recommendations each have been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact					
	Severe	High	High	Urgent	Urgent
	High	Medium	Medium	High	Urgent
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	High
		Remote	Unlikely	Likely	Very Likely
		Likelihood			

It is important to note that the above ratings are assigned based upon the ICO's assessment of the risks involved. LCC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

4. Audit opinion

The purpose of the audit is to provide the Information Commissioner and LCC with an independent assurance of the extent to which LCC, within the scope of this agreed audit, is complying with the DPA.

Overall Conclusion	
Reasonable assurance	There is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made one limited assurance assessment, in respect of data protection governance, and two reasonable assurance assessments, in respect of training and awareness and subject access requests, where controls could be enhanced to address the issues which are summarised below.

5. Summary of Recommendations

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 the DPA.	We have made **8** urgent priority recommendations across all 3 scope areas: **6** in data protection governance; **0** in training and awareness; and **2** in subject access requests where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the DPA.	We have made **39** high priority recommendations across all 3 scope areas: **15** in data protection governance; **11** in training and awareness; and **13** in subject access requests where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made **38** medium priority recommendations across all 3 scope areas: **13** in data protection governance; **11** in training and awareness; and **14** in subject access requests where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the data controller sees existing plans through to completion.	We have made **12** low priority recommendations across all 3 scope areas: **10** in data protection governance; **2** in training and awareness; and **0** in subject access requests where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

LCC have, since 2011, undertaken Information Security Risk Assessments at the outset of new or significant changes to data handling processes to identify and address information risks.

Employees must report all actual and suspected information security incidents to the Policy & Assurance Team (PAT).

Employees and agency workers must complete the Data Protection & Information Security training upon induction.

The PAT developed the content of the Data Protection & Information Security training and consulted ICO guidance when doing so.

LCC retain copies of subject access responses which may help to improve complaint handling.

LCC mark all subject access responses as 'data subject copy' which may help identify the source of any further disclosure of the information, should the need arise.

7.2 Areas for improvement

LCC have not established Key Performance Indicators (KPIs) to assist them in gauging and driving data protection compliance.

Only 63% of staff have completed the Data Protection & Information Security training.

LCC do not necessarily log subject access requests received outside of the central subject access team.

This page is intentionally left blank