ANNEX B

Nottinghamshire County Council

Data protection audit report

Executive summary
October 2015

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.

In January 2015, following a data security incident reported to the ICO, Nottinghamshire County Council (NCC) agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 24 June 2015 with representatives of Nottinghamshire County Council to identify and discuss the scope of the audit.

2. Scope of the audit

Following pre-audit discussions with Nottinghamshire County Council it was agreed that the audit would focus on the following areas:

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.

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

Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit opinion

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

The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA. We have made three limited assurance assessments where controls could be enhanced to address the issues.

4. Summary of audit findings

Areas of good practice

Information Asset Owners (IAOs) and the Senior Information Risk Owner (SIRO) have undertaken specialist role-based training, which was sourced by the Information Manager.

The Council ensures that Subject Access Requests (SARs) are valid by verifying requesters' identities and ensuring that those who make requests on behalf of another individual have a legal basis for doing so; e.g. they have the data subject's consent to request information or a legal power to do so, such as a power of attorney.

Complaints Information and Mediation Officers (CIMOs) peer review each other's SAR responses and Senior Practitioners conduct ad-hoc cold case reviews on SAR responses to ensure that they are appropriate.

The Multi Agency Safeguarding Hub (MASH) that the Council is involved in, has an appropriate Information Sharing Agreement setting out information sharing arrangements and responsibilities and an Information Security Protocol setting out the means by which information should be shared to ensure it is done in a secure way.

Areas for improvement

Information Governance training does not sufficiently cover key aspects of the Data Protection Act 1998 such as the eight principles, the recognition and handling of SARs and data sharing.

For many staff, Information Governance training is not carried out before they are granted access to personal data.

Key staff responsibilities in relation to SARs handling and corporate SAR response procedures have not been formalised within a corporate policy.

KPI's relating to SAR compliance are not currently reported to Board level to provide oversight and drive improvement.

The Council do not have a clearly defined corporate approach to data sharing; this is reflected in its lack of a corporate data sharing policy.

There is insufficient oversight of current data sharing arrangements and the Council has not identified all of the data sharing arrangements that are ongoing.

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 Nottinghamshire County Council.

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.