Appendix 1

Response from the Audit Commission

All firms in our audit regime are required to comply with all statutory and professional requirements when carrying out their role as appointed auditor. The requirements on appointed auditors regarding their access to, and use of information, are set out in the Audit Commission Act 1998 and the Commission's statutory Code of Audit Practice, which is supported by the Statement of Responsibilities of Auditors and Audited Bodies, and the Commission's Standing Guidance for Auditors. It is important to note that Section 49 of the Audit Commission Act makes it a criminal offence for appointed auditors, or their staff, to disclose information obtained in the course of an audit to third parties save in specified circumstances. The provisions of Section 49 must be drawn to the attention of all audit staff.

The Audit Commission considers appointed auditors to be data controllers in their own right for information collected in the course of their audit. This is consistent with guidance from the Information Commissioner's Office and the European Commission. Commission guidance to auditors is clear that only information strictly necessary for the purposes of the audit should be recorded within audit files and those files must be kept securely.

Where a firm wishes to process information overseas, they must in the first instance seek approval from the Commission to do so. Consent is given by the Commission, subject to five specific conditions, as set out below:

1. Whilst acting as a data processor for the purposes of the Data Protection Data Act 1998, firms shall take appropriate technical and organisational measures designed to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. In particular, firms will process personal data only for the purposes contemplated in agreement with the Commission and act on our instructions only (given for such purposes);

2. Firms shall comply at all times with the seventh principle in Part 1 of Schedule 1 to the Act as if applicable to the firm directly. Firms shall answer the Commission's reasonable enquires to enable the Commission to monitor compliance with this and firms shall not sub-contract the processing of personal data (unless to firm Persons who are required to take equivalent measures when processing personal data) without the Commission's prior written consent;

3. No government protectively marked data (being marked in accordance with the Government Protective Marking System as Top Secret, Secret, Confidential, Restricted or Protected*) will be involved;

4. No sensitive personal marked data (as defined by the Data Protection Act 1998) or protected personal data (as defined by the Cabinet Office Data Handling Review as 'any material that links an identifiable individual with information that, if released, would put them at a significant risk of harm or distress, or alternatively any source of information relating to 1000 or more

individuals is not considered likely to cause harm or distress') will be involved; and

5. Where relevant and appropriate the firm has notified audited bodies and relevant authorities.

**Please note this will change to "Top Secret, Secret or Protect: Sensitive" when the Government Protective Marking System changes, which is anticipated next year*.

The auditor of Leicestershire County Council is PwC LLP. You may find it helpful to know that the Commission has reviewed the information assurance arrangements of the firm and is satisfied as to its arrangements for the appropriate handling of Commission information, and also that the firm has received consent from the Commission to process information overseas, subject to the conditions set out above. You should be aware that these conditions are specific to where the auditor is acting as data processor on behalf of the Commission in its role as data controller. However, the Commission makes clear that it expects auditors to adopt the same standards when acting as data controller in their own right (e.g. when collecting data in the course of the audit).