Nottinghamshire County Council

APPENDIX C

DATA PROTECTION POLICY

CONTEXT

1. POLICY STATEMENT

1.1 The Data Protection Act 1998 ("**Act**") places legal responsibilities on Nottinghamshire County Council for the management of personal information.

1.2 Everyone has rights with regard to how their personal information is handled. During the course of its activities the Council will collect, store and process personal information about individuals ("**data subjects**") who have contact with it, and will recognise the need to treat that information in an appropriate and lawful manner.

1.3 The types of information that the Council may be required to handle include details of current, past and prospective employees, suppliers, customers, service users and others that the Council communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how the Council may use that information.

SCOPE OF THE POLICY

2. SCOPE

2.1 This policy has been approved by the Policy Committee. It sets out the Council's approach to data protection and the overarching legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The Council's Senior Information Risk Owner (SIRO) is responsible for ensuring compliance with the policy.

2.3 This policy applies to all personal data that the Council handles.

2.4 Elected members (reference to elected members in this Policy also includes co-opted members) and employees of the Council and any agency staff, contractors, consultants and partners that have access to

personal data held by or on behalf of the Council are required to be aware of this policy and have a responsibility to comply with it when handling personal data on behalf of the Council.

PRINCIPLES AND COMMITMENTS

3. DATA PROTECTION PRINCIPLES

Anyone processing personal information which relates to, and identifies, an individual (including an expression of opinion about such individual) ("**personal data**") must comply with the eight data protection principles. These provide that personal data must be:

(a) Processed fairly and lawfully;

(b) Processed for limited purposes and in an appropriate way;

(c) Adequate, relevant and not excessive for the purpose;

(d) Accurate;

(e) Not kept longer than necessary for the purpose;

(f) Processed in line with data subjects' rights;

(g) Secure;

(h) Not transferred to people or organisations situated in countries without adequate data protection measures.

4. COMPLIANCE

4.1 The Council shall endeavour to:

(a) Provide clear information to individuals about the purpose or purposes for which their information will be used, who it will be used by and for what purpose or purposes it will be shared with others;

(b) Only process relevant and adequate personal data;

(c) Keep personal data accurate and up to date;

(d) Retain personal data only for as long as necessary for legal, regulatory or legitimate Council purposes;

(e) Respect the rights of individuals in relation to their personal data, including their rights of access to records;

(f) Keep all personal data, in whatever format, secure;

(g) Take appropriate technical and organisational security measures to safeguard personal information;

(h) Only transfer information outside the European Economic Area in circumstances where it can be adequately protected;

(i) Ensure that third party processors of the Council's personal data have adequate controls and security measures in place;

(j) Acknowledge, investigate and respond to all complaints relating to a request for information;

(k) Develop guidance for its elected members and employees in order to help ensure awareness and compliance of the Council's obligations under the Act.

5. RETENTION OF DATA

Personal data will not be kept longer than is necessary for the purpose it was obtained. This means that data will be destroyed or erased from the Council's systems when it is no longer required.

6. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

Data will be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by the Council;

(b) Prevent the processing of their data for direct-marketing purposes;

(c) Ask to have inaccurate data amended;

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7. INFORMATION SECURITY

7.1 The Council will put in place appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

7.2 The Act requires the Council to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Where personal data is to be transferred to a third-party data processor, the third-party data processor shall be required to comply with those procedures and policies, or have in place their own adequate controls and security measures.

8. ACCESS TO RECORDS REQUESTS

8.1 A formal request from an individual for information that we hold about them ("**Access to Records Request**") must be made in writing. Access to Records Requests will be responded to within statutory timescales and the individual making the request may be charged a nominal fee for the provision of such information.

8.2 The Council shall maintain staff guidelines for identifying and dealing with Access to Records Requests. The guidance shall:

(a) explain how to identify and process a valid request;

(b) include up-to-date information about where to direct requests that are received and where to seek advice, should it be required;

(c) set out a process for handling complaints.

9. INFORMATION SHARING WITH PARTIES EXTERNAL TO THE COUNCIL

9.1 The Council may share personal data with outside organisations for a variety of different purposes, for instance, to allow the Council to comply with a legal requirement or for the purpose of carrying out public functions. Outside organisations, such as the police, may request that information is released to them on a one off basis for a particular purpose, for instance, a police investigation.

9.2 Where data sharing takes place or is contemplated between the Council and the same outside organisations on a regular basis, the Council shall consider entering into an information sharing agreement ("ISA") with those outside organisations.

9.3 ISAs produced by the Council shall include common provisions applicable to all parties participating in the ISA. The ISA should set out the legal basis for the sharing of personal data and explain how the data sharing will meet the requirements of the Data Protection Act. This should include:

(a) A description of the data to be shared;

(b) A description of measures to be taken to keep the data secure;

(c) A process for dealing with the reporting and management of breaches of the ISA;

(d) Detail how decisions regarding whether or not to share data are recorded;

(e) Details regarding how the quality of data is checked.

9.4 The Council shall maintain a process for reviewing and signing off ISAs. The process shall name who can sign off ISAs on behalf of the Council.

9.5 The Council shall maintain a register of information sharing agreements so that these may be monitored.

9.6 Personal data shall be shared in accordance with Council policy and guidance and in cases where there is an approved ISA in place, the relevant ISA.

KEY ACTIONS

10. NOTIFICATION

10.1 The Council has a statutory duty under the Act to provide Notification to the Information Commissioner about how it uses personal data. The Council will maintain a Notification that it will regularly review and update as necessary.

11. TRAINING AND AWARENESS

11.1 The Council shall make provision for information governance training and will maintain a record of employees who have received training.

11.2 The Council shall ensure that appropriate training is provided to employees who handle personal data in order to effectively manage risks.

11.3 Awareness of this policy shall be promoted to all elected members, employees, contractors and temporary staff through the Council's intranet, team briefings and general communications material.

12. FAIR PROCESSING NOTICES

12.1 Where personal data is collected for more than one purpose (primary and secondary uses) or is shared with outside organisations; the Council shall ensure as far as possible that the data subject is made aware of this through the provision of a fair processing notice which should be provided at the time the personal data is collected.

MONITORING AND REVIEW OF THE POLICY

13. REVIEW PROCESS

13.1 This policy is to be kept under review by the Senior Information Risk Owner on a biennial basis with the next review being scheduled for April 2018. Recommendations for any material amendments will be approved by Policy Committee.

Document control

Owner:	Team Manager, Complaints and Information
Approved by:	Policy Committee
Date:	20 April 2016
Review/Amendments	[March 2016] - Policy updated to reflect new reporting requirements and includes new sections on information sharing, privacy notices and training.