NUNEATON AND BEDWORTH BOROUGH COUNCIL

DATA PROTECTION ACT 1998

DATA PROTECTION POLICY

NOVEMBER 2012

Report Control Information

Title: Data Protection Policy

Date: November 2012

Version: 1.0

Reference: X540.2

Author: Wendy Davies-White

Director: Philip Richardson – Director Governance and Recreation

Managing Director Alan Franks

REVISION	DATE	REVISION DESCRIPTION
1	2005	Approved
1	2012	Update – Approved 29.01.13 IC538

Contents Page

Nuneaton and Bedworth Borough Council

Data Protection Policy

1 Introduction

Nuneaton and Bedworth Borough Council ("the Council") is committed to full compliance with the Data Protection Act 1998 ("the Act") which came into force on 1st March 2000. The Council will therefore follow procedures designed to provide that all elected members, employees, contractors, consultants, partners, or other servants or agents of the Council (collectively referred to as "the data users") who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the Act.

In order to operate efficiently, the Council, as Data Controller, has to collect and use information about people with whom it works. The definition of personal data is set out in APPENDIX A. The personal data is held in a variety of formats, electronic and manual. The Council is as far as practicable open about the type and extent of personal data that it holds and as a responsible body is committed to ensuring that information is handled and dealt with properly and that it maintains the best possible security and confidentiality of personal data.

It will take all necessary steps to ensure that personal data held by the Council about its employees, customers, suppliers and other individuals (collectively referred to as "the data subjects") is processed in accordance with the Data Protection Act 1998 ("The Act") and Principles. The definition of processing, and The Principles are set out in APPENDIX A of this Policy.

2 Co-ordination of Data Protection Issues

Each Service Unit will identify an officer (the data protection officer) with responsibility for co-ordinating all data protection issues for that Unit, and liaising with the Director – Governance & Recreation to ensure that the Council's Notification to the Information Commissioner (the Commissioner) is kept up-to-date, for the receipt of subject access requests and the co-ordination of and compliance with the requirements of the Act when such requests are received.

3 Duties of Data Protection Officer

The officer shall ensure that:

(a) All purposes for which personal data is obtained or processed is notified to the Commissioner as required by the Act.

(b) No personal data is obtained, held or processed, for any purpose, without that purpose being notified to the Commissioner as required by the Act.

(c) All data is processed fairly and lawfully, unless such processing is exempt under section 29 of the Act (crime and taxation). In particular, form and document design will be kept under review, to ensure compliance with the data protection principles under the Act.

(d) All processing of personal data is subjected to a risk assessment, taking into account:

(i) the likelihood of a breach of the data protection system;

(ii) the potential impact on the data subject, elected members or employees and

(iii) the level of controls in place with regard to the data, together with the setting and testing of clear controls to minimise breaches of the Act.

(e) No disclosure of data is undertaken by any data user which breaches any of the provisions of the Act, as interpreted by the Council, the Commissioner or the courts for the time being.

4 Training

The Council will take measures to ensure that data users and elected members are fully trained in and aware of this policy and their duties and responsibilities under the Act.

5 Breach of the Act

The attention of all employees and elected members will be drawn to the requirements of the Act and procedures laid down by The Council to ensure compliance. It is the duty of employees to comply with the procedures and to co-operate with this Policy. The Council regards any unlawful breach of any provision of the Act by any employee of the Council as being a disciplinary matter. Any employee(s) who breach this policy will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Breach of the policy by an elected member will be dealt with pursuant to the Members Code of Conduct.

6 Service – Related Policies

Each Service Unit of the Council will compile and maintain a combined Data Protection Policy and Code of Practice, which will be subordinate to this policy and will be advertised and available for public inspection. Such policies and codes of practice shall incorporate procedures for the weeding, deleting and destruction of personal data to ensure compliance with the third, fourth, fifth and seventh data protection principles under the Act.

Each Manager will have immediate responsibility for data protection matters in his/her service unit.

7 Audit and Review of Data Protection System

The Council will undertake a rolling audit and review of all data protection systems and controls to ensure compliance with the Act, this policy and individual service data protection policies and codes of practice, including data security.

8 Duties of Contractors and Partners

All contractors, consultants, partners, or other servants or agents of the Council must:

(a) Ensure that they and all of their employees who have access to personal data held or processed for or on behalf of the Council are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm.

(b) Promptly, pass any subject access requests relating to the Council's business to the appropriate Data Protection Officer and provide that person with any information needed by them to comply with the subject access request.

(c) Allow data protection audits by the Council of data held on its behalf.

(d) Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

The Council will monitor ongoing compliance with the Act by third party processors of data.

9 Requests for Access to Personal Data

(a) The Council will ensure as far as practicable that the rights of individuals as set out in the Act are maintained and upheld. Under s 7(1) of the Act individuals have a right of access to personal data held about them by the Council, subject to limited exemptions.

This is called the **"Right of subject access".** Upon making a request in writing and upon paying the fee to the Council an individual is entitled to be told by the Council whether it or someone else on its behalf is processing that individual's personal data, if so, to be given a description of:- i) the personal data, ii) the purposes for which they are being processed, and iii) those to whom they are or may be disclosed. Individuals are entitled to receive a copy of the personal data held about them. Subject Access Requests must be complied with within 40 days of receipt and specifically request personal data. Other requests for information from the Council should be dealt with in accordance with the Freedom of Information Act 2000, in respect of which the Council has separate policies and procedures.

(b) To ensure full compliance with the requirements of the Act protocols and procedures will be set and annually tested to ensure the authority's ability to respond to individual access requests promptly and, in any event, within the timescales laid down in law.

(c) Any orders or requests for disclosure of personal data, which are deemed to fall under one of the categories of exemptions under sections 27 to 37 of the Act, or under any other statutory power shall be passed promptly to the data protection officer within the relevant Service Unit, who will be responsible for and take reasonable steps to ensure that the request does fall within the relevant exemption and comply with the request in a manner deemed by that person to be appropriate.

10 Security of Data

All data users will ensure that appropriate security measures are undertaken to safeguard personal data, commensurate with the nature of the data concerned.

The unlawful disclosure of information is a criminal offence under the Act.

11 Notification

The Information Commissioner maintains a public register of data controllers. The Council is registered with the Information Commissioner. The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

The annual renewal is undertaken by the Director – Governance & Recreation. Data Protection Officers within every service unit will be responsible for liaising with the Director – Governance & Recreation to ensure that the notification is up to date for their Service Unit.

Any changes to the Register must be notified to the Information Commissioner within 28 days. Any changes to processing carried out within a service unit must be brought to the attention of the Director – Governance & Recreation immediately.

12 Queries

Any questions regarding this Policy or Data Protection is general should, in the first instance be directed to the relevant Data Protection Officer for the Service Unit. The Principal or Senior Solicitors should be contacted for further assistance.

Further advice and guidance can be obtained from the Information Commissioner's website http://www.ico.gov.uk

This Policy will be reviewed every three years

This Policy was adopted by minute of 2012

Appendix A

Definition of Personal Data

Personal data is defined as data relating to a living individual who can be identified from

- The data

- That data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or ant other person in respect of the individual.

Definition of Processing

In this policy document, the term “processing” means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available,

(d) or alignment, combination, blocking, erasure or destruction of the information or data and “processed” shall be construed accordingly.

Data Protection Act 1998 Principles

First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- **at least one of the conditions in Schedule 2 is met, and**

- **in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**

- as set out in Appendix B.

Therefore those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

Personal data shall be accurate and, where necessary, kept up to date. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the Authority are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the Authority of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Authority to ensure that any notification regarding change of circumstances is noted and acted upon.

Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Personal data shall be kept only for as long as necessary. See the Council's Retention Policy.

Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

This includes:-

- the right to be informed that processing is taking place

- the individuals right to receive a copy of data held about him within 40 days of request

- the right to prevent processing in certain circumstances

- the right to correct, rectify, block or erase information regarded as incorrect

- to request the Commissioner to assess whether any provision of the Act has been contravened

Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All necessary steps must be taken to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular measures will be put in place to ensure that paper files and other records and documents are kept in a secure environment; personal data held on computer is protected by the use of secure passwords.

Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Appendix B

Conditions for Processing - Schedules 2 and 3 of the Data Protection Act 1998

Conditions for Processing Data - Schedule 2

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):-

- The data subject has given their consent to the processing
- The processing is necessary:-
    a) for the performance of a contract to which the data subject is a party, or
    b) for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The processing is necessary in order to protect the vital interests of the data subject.
- The processing is necessary:-
    a) for the administration of justice,
    b) for the exercise of any functions conferred by or under any enactment,
    c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
    d) for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Conditions for Processing Sensitive Data (Schedule 3 of the Act)

Sensitive Data is defined by the Act as personal data consisting of information as to:

b) the racial or ethnic origin of the data subject

c) their political opinions

d) their religious beliefs or other beliefs of a similar nature

e) whether they are a member of a trade union

f) their physical or mental health or condition

g) their sexual life

h) the commission or alleged commission by them of any offence or

i) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

At least one of these must be satisfied, in addition to at least one of the conditions for processing in Schedule 2 (which apply to the processing of all personal data), before processing of sensitive personal data can claim to have been lawful in accordance with the first Principle.

- The data subject has given their explicit consent to the processing of the personal data

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.

- The processing is necessary-

  a) in order to protect the vital interests of the data subject or another person, in a case where:-

     i) consent cannot be given by or on behalf of the data subject; or

     ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

  b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- The processing:-

  a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes and which is not established or conducted for profit,

  b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and

d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

- The processing is necessary:-

  a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

  b) for the purpose of obtaining legal advice, or

  c) for the purposes of establishing, exercising or defending legal rights.

- The processing is necessary:-

  a) for the administration of justice

  b) for the exercise of any functions conferred by or under any enactment, or

  c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

The Secretary of State has by order specified cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.