Nottingham City Council

Title: Data Protection Policy

Approved By	Information Management Strategy Group
Approval Date	16 February 2015
Review Date	Annual
Disposal Date	Ongoing subject to review
Version History	V2.4 (2015) Full version history on following page
Contact for further information	Stephanie Pearson, Information Management, Development Stephanie.pearson@nottinghamcity.gov.uk 011 876 3164
Confidentiality	UNCLASSIFIED

Version Control page

Title: Data Protection Policy

Current version: Version 2.3

Document type: Full Policy Document

Authored by: Stephanie Pearson, Information Specialist
Approved by: Information Management Strategy Group – 16 Feb 2015
Review date: Annual - February 2016
Circulation: All employees and customers upon request and via the website

Document revision dates

Revision	Date	Revision description
Version 2.3	February 2015	Minor revisions made to reference templates/procedural/guidance documents not yet written but aspired to be, and firm references made to Information Asset register. Again guidance on this has not yet been drafted/approved.
Version 2.2	February 2015	Minor revisions to reference all new templates/procedural/guidance documents linked to policy
Version 2.1	December 2013	Minor revision – disproportionate effort exemption removed in accordance with revised ICO guidance.
Version 2.0	June 2009	Complete Revision and separation from Access Policy
Original – Access Policy	December 2004	Access Policy produced by A Stead – approved SMT January 2005.

NOTTINGHAM CITY COUNCIL

DATA PROTECTION POLICY

Nottingham City Council recognises its obligations to comply with the requirements laid down in the Data Protection Act 1998 (DPA).

This policy should be read in conjunction with the relevant sections of the Information Governance Procedure Manual on DPA and all associated templates, procedures and guidance notes.

1. Introduction.

Nottingham City Council ('the Council') aims to ensure that personal information is treated lawfully and correctly. The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the Council deals and in achieving its objectives.

The Council fully endorses and adheres to the Data Protection principles set out below:-

THE EIGHT DATA PROTECTION PRINCIPLES
Personal Information:

- shall be processed fairly and lawfully and shall not be processed unless specific conditions are met;
- 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;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- shall be accurate and where necessary kept up to date;
- shall not be kept for longer than is necessary for that purpose or those purposes;
- shall be processed in accordance with the rights of data subjects under the Act;
- appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- shall not transfer personal data 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.

2. Policy Aim

To ensure the Council complies with all relevant legislation and good practice to protect all of the personal information that it holds.

3. Policy Objectives

To achieve the overall aim the Council will:

3.1 Provide adequate resources to support an effective corporate approach to data protection.
3.2 Respect the confidentiality of all personal information irrespective of source.
3.3 Publicise the Council's commitment to Data Protection.
3.4 Compile and maintain appropriate procedures and codes of practice.
3.5 Promote general awareness and provide specific training, advice and guidance to its staff at all levels and to its Members to ensure standards are met.
3.6 Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

4. Processing of Information:

The Council, through appropriate management controls will, when processing personal information about any individual:

4.1 Observe fully the conditions regarding the collection and use of information and meet the Council's legal obligations under the Data Protection Act 1998 ('the Act').
4.2 Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.
4.3 Ensure that the individual about whom information is held can exercise their rights under the Act, including:-
  4.3.1 the right to be informed that processing is being undertaken
  4.3.2 the right to prevent processing in certain circumstances
  4.3.3 the right to correct, rectify, block or erase information, which is regarded as incorrect information.
  4.3.4 the right of access to personal information

5. Access to Personal Information

Nottingham City Council will process requests for access to personal information in line with the relevant sections of the Data Protection Act 1998.

5.1 Subject Access (Section 7) Requests:

A member of the Information Governance team authorised by the Council will assess every request for access to personal data to establish;

- if the request is a valid subject access request or if more information is required from a requester;
- if more information is required this will be requested from the requester;
- if all information has been received, the Council will acknowledge the request and process the request within 40 calendar days from receipt;

5.2 Other Access Requests:

- Requests from any external agency or Data Controller will be processed in accordance with section 29 or 35 of the Data Protection Act 1998, or where this is not possible in accordance with the relevant Schedules.
- An appropriately authorised employee of the Council will ensure that any disclosure made without the consent of the subject is done so in accordance with all other legislation, taking account of an individual’s rights as enshrined in the Human Rights Act 1998.

6. Fair Obtaining/Processing

Individuals whose information is collected by the Council must be made aware at the time of collection of all the processes that data may be subject to. No manual or

automatic processing of an individual's personal information should take place unless reasonable steps have been taken to make that individual aware of that processing. Individuals must also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information.

The Councils Fair Processing Notice templates and Guidance must be adhered to, and if any change of use is being made to data, or a new project or system being initiated or procured, then the Council advocates that a Privacy Impact Assessment is conducted using the relevant Council template and guidance.

7. Data Uses and Purposes

7.1 All processing of personal data must be for a purpose that is necessary to enable the Council to perform its duties and services, and which has been notified by the Council to the Information Commissioner. Personal information should only be processed in line with those notified purposes. If processing is required for a reason not already registered with the Information Commissioners Office, our registration should be amended prior to this type of processing taking place.

7.2 No new processing should take place UNTIL the Information Commissioner has been notified of the relevant purpose AND the data subjects have been informed and, in the case of sensitive data, their consent obtained. All new occurrences of, or future developments for, processing of personal data must therefore be reported to the Information Management Service, which is responsible for maintaining the Council's Data Protection notifications. It is also likely that a Privacy Impact Assessment will need to be undertaken.

7.3 All personal data should be regarded as confidential and its security protected accordingly. This also applies when Council information is being processed at employees' homes. Employees should only remove personal information from a Council office with the authority of their line manager, Head of Service or the Chief Executive. Any misuse, loss or unauthorised disclosures while the information is in their control may result in disciplinary proceedings. Information held by the Council must not be used for unauthorised non-Council purposes. If you become aware of any potential data breach, please refer to section 9 below, and follow the designated procedures accordingly.

7.4 Personal Information should only be disclosed to persons (internal and external) who are listed for the purpose concerned in the Council's current notification OR where their authority to receive it has been explicitly established, e.g. where the information is required by the police for the prevention and detection of crime, or a relevant Information Sharing Agreement, (using the Councils Information Sharing Template and guidance), is in place.

8. What counts as Personal Information?

This is any information held by the Council about a living individual, from which that individual can be identified. For example, this will include:

- A name and address,
- information attached to a reference number that could be used to identify someone

- a company e-mail address if it includes a person's name.

9. Data Breaches

Employees must notify the Information Management Services Team of any potential data breaches using the procedure articulated on the Information Matters intranet pages:

http://gossweb.nottinghamcity.gov.uk/nccextranet/index.aspx?articleid=17810.

Any reported data breach will be investigated to ascertain whether it is more an information or IT security related matter, the incident will then be progressed accordingly. Information Management Services and IT will then work together to initially retrieve any missing data and prevent the same incident occurring again, and will then look to implement lessons learned across the wider organisation.

If a member of the public reports a potential breach, they can do this by contacting Information management Services directly on 0115 87 63855 or by e-mailing information.governance@nottinghamcity.gov.uk

For members of the public, further information can be found on our webpages at:

http://www.nottinghamcity.gov.uk/article/24515/Access-to-Information

10. Data Quality

Information processed should not be excessive or irrelevant to the notified purposes. Information must be held only for so long as is necessary for the notified purposes, after which it should be deleted or destroyed in accordance with the Council's Retention and Disposal Schedule (now incorporated into the Council's Information Asset Register (IAR) see below). Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

11. Information Asset Register (IAR)

In order to be able to properly and effectively comply with our obligations under the Data Protection Act, the Council needs to fully understand what information it holds and where this information is kept. We also need to consider how we keep this information up-to-date and how we know when to dispose of it. The Council's Information Asset Register is a tool which should allow us to do all of these things more effectively. The Council's IAR is currently being compiled. This IAR does not hold the data or information itself, but the metadata about the information. The Council's Information Asset Register will:

- Identify and describe Information Assets, and their role in the business
- Name the systems Information Assets are held in
- Set out the ownership, governance and maintenance of Information Assets

- Set out how access to Information Assets is controlled
- Set out retention and disposal schedule for Information Assets.

Information Asset Owners are responsible for maintaining an entry of all information assets used in their business area in the Information Asset Register. For further information on the Information Asset Register and colleagues responsibilities, please see the 'Information Asset Register Guidance' or visit the Information Matters intranet pages.

12. Organisational Responsibilities and Security

The Council is obliged under the Act to ensure that all appropriate technical and organisational measures are taken to safeguard against unauthorised or unlawful processing of personal information and against the accidental loss, damage or destruction of personal information.

12.1 All personal information must be kept secure, in a manner appropriate to its sensitivity and the likely harm or distress that would be caused if it was disclosed unlawfully. To ensure that an appropriate level of security is afforded to all information the Council's Information Security policy will be adhered to at all times.

12.2 Everyone managing and handling personal information will be appropriately trained to do so.

12.3 All members of staff have a duty to follow this Policy and associated procedures and to co-operate with the Council to ensure that the aim of this Policy is achieved.

12.4 Disciplinary action may be taken against any member of staff who fails to comply with or commits a breach of this Policy.

12.5 It is the duty of individual members of staff to ensure that personal information held by them is dealt with in accordance with the Act.

12.6 Suitable measures should be taken to ensure that any processing of personal data carried out by a third party on behalf of the Council complies with the Principles of the Act and this Policy. Similarly, when the Council is processing personal information on behalf of a third party it will need to demonstrate that the information is subject to the same standard of care.

Relevant templates/guidance and procedures to which this policy refers:

All of the Council's Data Protection information can be accessed by colleagues via the Information Matters website. This website includes (but is not limited to) the following key documents

- NCC Privacy Impact Assessment Template and Guidance
- NCC Fair Processing Notice Templates and Guidance
- NCC Information Sharing Agreement Template and Guidance
- NCC Data breach and IT Incident Reporting Procedure

http://gossweb.nottinghamcity.gov.uk/nccextranet/index.aspx?articleid=17449

A further suite of associated policies, templates, procedural and guidance documents will be developed, each of which will also be reviewed annually, and amended as the need arises. Supporting documents will be endorsed by the IMSG, and will include (but not be limited to):

- Information Governance Framework
- Records Management Policy
- Security policy
- Email policy
- Acceptable Use policy
- Information Asset Register Guidance
- Information security Classifications Policy
- Information security Classifications Guidance