Data Protection Policy

DOCUMENT PROVENANCE			
Status	Approved	Current version no.	3.1
Organisation	Nottingham City Council	Version date	2018-04-24
Author	Naomi Matthews	Approved by (If applicable)	
Audience	Anyone	Approval date	
Security classification	OFFICIAL	Next review date	Annually

DOCUMENT CHANGE HISTORY			
Revision date	Version no.	Author of changes	Summary of changes
2004-12	1.0	A Stead	Original Policy. Also included access policy
2009-06	2.0	S Pearson	Complete revision and separation from Access policy
2013-12	2.1	S Pearson	Minor revision-disproportionate effort exemption removed in line with ICO guidelines
2015-02	2.2	S Pearson	Minor new revisions to reference all new templates/ procedural/ guidance documents linked to policy
2015-02	2.3	S Pearson	Minor revisions to reference all new templates/ procedural/ guidance documents linked to the policy
2016-03	2.4	S Pearson	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.
2017-06	2.5	J Locker	Review
2017-09	2.6	N Matthews	Review
2017-12	3.0	N Matthews	Complete revision in line with the GDPR and DPA 2018
2018-04	3.1	N Matthews	Minor revisions
2019-03	3.2	N Matthews	Minor revisions

Contents

1. Introduction 3
2. Definitions 3
3. Policy Aim 4
4. Policy Objectives 4
5. Processing of Information 5
6. Processing of special categories of personal Information 5
7. Access to Personal Information 6
8. Fair Obtaining/Processing 7
9. Data Uses and Purposes 7
10. What counts as Personal Information? 8
11. Data Incident Reporting/ Data Breach 8
12. Data Quality and Retention 8
13. Records of processing activities 9
14. Data Security 9

Nottingham City Council recognises its obligations to comply with the requirements laid down in the General Data Protection Regulation (GDPR) ((EU) 2016/679 and any national implementing laws, including the Data Protection Act 2018.

This policy should be read in conjunction with the Appropriate Policy Document, the Data Breach, Personal Information Procedure and Guidance, Records Management and Retention Policy, associated templates, procedures and Information Commissioners Office 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. This policy sets out the basis on which the Council shall process any personal data from citizens, staff and other parties from whom data is collected.

The Council, and therefore any person who handles personal data on behalf of the Council, fully endorses and adheres to the Data Protection principles set out in Article 5 of the GDPR and shall be responsible for, and be able to demonstrate, compliance with the principles outlined below:-

THE SEVEN DATA PROTECTION PRINCIPLES

Personal Information shall be:

- processed lawfully, fairly and in a transparent manner **(lawfulness, fairness and transparency)**
- collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes; **(purpose limitation)**
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; **(data minimisation)**
- accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **(accuracy)**
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (**storage limitation**)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**)
- The controller shall be responsible for, and be able to demonstrate compliance with all six principles above (**accounatability**)

Personal Data

Means any information relating to an identified or identifiable natural person (data subject) an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the

physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal data breach

Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed

Consent

Means any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.

Special categories of personal data

Is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation.

Processing

Includes any operation or set of operations, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration,

Personal Information Request (previously known as a Subject Access Request)

Right to access to the personal data by the data subject (e.g. the citizen or member of staff).

Data Subject

This will be the person that we collect the data from. This will include citizens, and members of staff.

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:

4.1 Provide adequate resources to support an effective approach to data protection.
4.2 Respect the confidentiality of all personal information irrespective of source.
4.3 Publicise the Council's commitment to data protection.
4.4 Compile and maintain appropriate procedures and codes of practice.
4.5 Promote general awareness and provide specific training, advice and guidance to its staff at all levels to ensure standards are met
4.6 Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary

4.7 Monitor, ensure and report on compliance with this policy and the GDPR and Data Protection Act 2018 through an assurance framework which will include training and be reported quarterly to the Information Compliance Board and at least annually to the Audit Committee.

4. Processing of Information

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

5.1 Observe fully the conditions regarding the collection and use of information and meet the Council's legal obligations under the GDPR and the Data Protection Act 2018.

5.2 Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

5.3 Ensure that the individual about whom information is held can exercise their rights under the GDPR and the DPA Act 2018 unless an exemption applies. including:-

- the right to be informed that processing is being undertaken
- the right to prevent processing in certain circumstances
- the right to correct, rectify, block or erase information, which is regarded as incorrect information
- the right of access to personal information
- the right to erasure
- the right to portability where applicable.

5. Processing of special categories of personal Information

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

6.1 Shall observe fully the conditions regarding the processing of special categories of information as outlined in Article 9 and meet the Council's legal obligations under the GDPR and the Data protection Act 2018. In particular, Schedule 1 Part 4 of the DPA 2018 states that the Council must have this policy document in place which explains as below, the procedures for securing compliance with the principles in Article 5 as outlined above.

6.2 Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

6.3 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs data, data concerning health or data concerning a natural person or trade union membership and the processing of

genetic data biometric data for the purpose of uniquely identifying a natural person,

6. Processing by Third Parties

Nottingham City Council as data controller will implement appropriate technical and organisational measures to ensure compliance with this policy and the GDPR and Data Protection Act 2018. This will include but not be limited to:

7.1 Performing a Data Protection Impact Assessment (DPIA) before selecting a third party processor where the processing is likely to result in a high risk to the rights and freedoms of citizens.
7.2 Performing checks on potential third party processors to ensure their suitability for the role.
7.3 Entering into a contract with the third party which sets out the relationship, roles and responsibilities of the data controller and processor.
7.4 Ensuring that such contracts comply with best practice and are recorded on the corporate contracts register by working with the procurement team in procuring the data processing contract.
7.5 Updating the Information Asset Register where appropriate.
7.6 Monitoring and contract management to obtain assurance that the third party is complying with its contractual and legal obligations, including data breach notifications.

7. Access to Personal Information

Nottingham City Council will process requests for access to personal information in line with the relevant sections of the GDPR and the Data protection Act 2018.

7.1 **Personal Information Requests/ Subject Access requests:**

Individuals can request a copy of the personal data that the Council holds about them. Any staff member who receives a valid data protection request must forward it to the Information Compliance Team.

- if the request is a valid subject access request, the Information Compliance Team will acknowledge the request and process the request
- if more information is required this will be requested from the requester;
- if all information has been received, the Information Compliance Team will acknowledge the request and process the request within one month from receipt; unless the request is particularly large and complex in which case the time can be extended for two months.

7.2 **Requests from other agencies for personal information:**

- Requests from any external agency will be processed in accordance with the GDPR and Data Protection Act 2018.
- An appropriately authorised employee of the Council will ensure that any disclosure made without the consent of the data subject is done so in accordance with all DPA legislation and other relevant legislation, taking account of an individual's rights as enshrined in the Human Rights Act 1998.

8. 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 data subjects will also be informed of the purposes of the processing as well as the legal basis for processing. They should also be provided with the Data Protection Officer's details.

Information will also be provided as to how long the information will be kept for, the rights that data subjects can exercise with regards to their data and information to enable data subjects to lodge a complaint with the Information Commissioners office if their rights are not met under the GDPR and DPA 2018.

9. Data Uses and Purposes

9.1 All processing of personal data must be for a purpose that is necessary to enable the Council to perform its duties and services. Personal information should only be processed in line with those notified purposes.

9.2 All personal data should be regarded as confidential and its security protected accordingly. This also applies when Council information is being processed at employee's 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 11 below, and follow the designated procedures accordingly.

9.3 Personal Information should only be disclosed to persons (internal and external) 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 is in place.

9.4 Purposes will include the following:

- To allow the Council to be able to communicate and provide services appropriate to the citizen's needs, e.g. to be able to arrange suitable access arrangements where the citizen has mobility difficulties
- To ensure that the council meets its legal requirements, including obligations imposed under the Race Relations Act and Health and Safety Act
- Where necessary for the Council's Law Enforcement functions, e.g. licensing, planning enforcement, trading standards, food safety, etc.
- Where Nottingham City Council is legally obliged to undertake such processing for the purpose for which the data subject provided the information, e.g. processing information given on a benefit claim form for

the purpose of processing a benefit claim, and to monitor the Council's performance in responding to the citizen's request

- Where the processing is necessary for Nottingham City Council to comply with its legal obligations, e.g. the prevention and/or detection of crime
- To process financial transactions including grants, payments and benefits involving Nottingham City Council, or where Nottingham City Council is acting on behalf of other government bodies, e.g. Department for Works and Pensions
- Where the citizen have consented to the processing
- Where necessary to protect individuals from harm or injury
- Where otherwise permitted under the GDPR and the Data Protection Act 2018, e.g. disclosure to comply with legal obligations
- Nottingham City Council may also use a citizens personal data, after it has been anonymised, to allow the statistical analysis of data to allow the Council to effective target and plan the provision of services.
- Safeguarding and promoting the welfare of children
- Providing human resources function for staff

10. 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 directly or indirectly
- a company e-mail address if it includes a person's name

11. Data Incident Reporting/ Data Breach

Employees must notify the Information Compliance Team of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence by contacting information.compliance@nottinghamcity.gov.uk

Any reported data incident will be investigated appropriately with the relevant stakeholder(s) and actions taken as necessary.

If a member of the public reports a potential incident, they can do this by contacting the Data Protection officer directly on 0115 8763855 or by e-mailing information.compliance@nottinghamcity.gov.uk

Personal data breaches will be notified to the Information Commissioner's Office within 72 hours of the incident. All staff members will follow the Data Breach guidance manual and associated templates, procedures and the Information Commissioners Office guidance.

12. Data Quality and Retention

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 and contained in the Councils record management policy. Retention periods where possible shall be found in the records of processing and the Council must ensure that this is kept up to date and that the retention periods are acted upon unless there is a reason not to do so.

Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

13. Records of processing activities

In order to be able to properly and effectively comply with our obligations under the GDPR and the DPA 2018, 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 shall maintain a record of processing which include the following information:

- The name of the Council and the details of the Data Protection Officer
- The purposes of processing as outlined above in this policy document
- Which condition is relied on and in particular, how the processing satisfies Article 5 and 6
- Set out the ownership, governance and maintenance of Information Assets
- Set out retention and disposal schedule for Information
- Sets out whether the personal data is retained and erased in accordance with the policy and if it is not the reason for not following the policy
- Map the flow of data in and out of the teams within the Council.

14. Data Security

The Council is obliged 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.

14.1. 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 Councils' Information Security policy will be adhered to at all times.

14.2. Everyone managing and handling personal information will be appropriately trained to do so and this will include appropriate refresher training every year.

14.3. 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.

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

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

The Data Protection Policy should be read in conjunction with the following:

- Records Management Policy
- Email policy
- IT Acceptable Use policy
- Data Breach Guidance
- Personal Information Requests Guidance
- Privacy Notice guidance
- Absent User Requests guidance