Data Protection Policy

Contents

Version	Amended by	Date	Summary
1.0		May 2018	
2.0	HIAG	January 2023	

1. Scope

1.1 This Policy applies to:

1.1.1 All Employees of the Council;
1.1.2 Members of the Council;
1.1.3 Suppliers and Contractors of the Council;
1.1.4 Temporary Staff engaged by the Council;
1.1.5 Volunteers at the Council;
1.1.6 All others using the Council's Information or Systems.

1.2 The Policy applies to all information which is subject to the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) including:

1.2.1 all personal data that is processed automatically;
1.2.2 any personal data held in a manual form in a relevant filing system;
1.2.3 any personal data held in an accessible record.

1.3 ***Personal Data*** *is defined by Article 4 of the UK GDPR as "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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*

1.4 ***Special Category Personal Data*** *is defined by Article 9 of the UK GDPR as "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 purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."*

1.5 Special Category Personal Data can only be processed by the Council if one or more specified statutory conditions apply. For the avoidance of doubt, they are not the conditions referred to in paragraph 5.3 below. Legal advice should be sought if any information about the statutory conditions relating to special category personal data is required.

2. Purpose

2.1 This Policy provides important information to all Council Staff and Managers about keeping data safe and secure and other responsibilities necessary to meet the requirements of the DPA and the UK GDPR. All those accessing or processing personal data in connection with Council business are individually responsible for ensuring that they comply fully with the DPA and the UK GDPR.

2.2 All staff have a responsibility at work to look after personal data properly and appropriately. Residents and other members of the public with whom the Council deals with have a right to know that information about them is kept secure.

2.3 Breaches of the DPA and the UK GDPR, through loss or mishandling of personal data, can result in large fines for the Council up to £17.5 million. The Council will also suffer significant reputational damage.

2.4 Individual members of staff can also face disciplinary action for misusing personal data they have access to as part of their employment with the Council.

2.5 The Council recognises that its residents value their privacy and it is committed to achieving strong levels of data protection. This is part of the Council's ethos of putting residents first.

2.6 The Council will:

2.6.1 provide adequate resources to support an effective corporate approach to data protection;
2.6.2 respect the confidentiality of all personal information irrespective of source;
2.6.3 compile and maintain appropriate procedures;
2.6.4 promote general awareness and provide specific training, advice and guidance to staff at all levels and to Members, to ensure that statutory requirements and good practice are met; and
2.6.5 monitor and review compliance with legislation and good practice guidance and introduce changes to policies and procedures where necessary.

2.7 Staff should not process any personal data unless they are certain that they are authorised to do so. Failure to comply with this Policy or any associated data protection policy, procedure or guidance may lead to action under the Council's disciplinary procedure.

2.8 All Council employees and contractors will be responsible for compliance with this Policy, the DPA and the UK GDPR.

3. The Statutory Data Protection Officer

3.1 In accordance with Article 37 of the UK GDPR, the Council has to appoint a Statutory Data Protection Officer (DPO).

3.2 The DPO is responsible for ensuring Council compliance with the DPA and the UK GDPR and does not receive any instructions regarding the exercise of his statutory duties. The DPO shall not be dismissed or penalised by the Council for performing his statutory duties which include:

3.2.1 to inform and advise the data controller or the processor and the employees who carry out processing of their obligations pursuant to the UK GDPR;
3.2.2 to monitor compliance with the UK GDPR and the DPA and with this Policy and other data protection procedures and policies.
3.2.3 to provide advice where requested as regards Data Protection Impact Assessments and monitor their performance.
3.2.4 to act as the contact point for the Information Commissioners Office (ICO) on all matters relating to data protection.
3.2.5 to cooperate fully with the ICO.

3.3 The DPO is Glen Egan – Acting Head of legal Services & Monitoring Officer who reports directly to the Chief Executive. His contact details are:

Email: GEgan2@Hillingdon.Gov.UK Telephone: 01895 277602

4. Staff Training and Guidance

4.1 Training and induction for staff includes data protection training. There are regular updates provided to all staff.

4.2 Where staff work in areas that deal with personal data on a regular basis, successful completion of data protection training is compulsory before staff are permitted to access and handle any personal information.

4.3 Regular briefings on data protection are provided to Managers.

4.4 All Council employees are required to complete the data protection module.

5. About the DPA & UK GDPR

Data Protection Principles

5.1 The following 6 Data Protection Principles are set out in the UK GDPR and the DPA and provide the framework for this Policy:

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are accurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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; ('storage limitation');

(f) 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').

5.2 The data controller (the Council) shall be responsible for, and be able to demonstrate compliance, with these Principles

Lawfulness of Processing

5.3 Personal data can only be lawfully processed if one or more of the following conditions apply (and which is set out in the Lawful Basis for Processing of Personal Data Policy below):

a) data subject has given consent;
b) processing is necessary for the performance of a contract which the data subject is party to;

c) processing is necessary for compliance with a legal obligation to which the data controller is subject;
d) processing is necessary to protect the vital interests of the data subject or another person;
e) processing is necessary for the performance of a task carried out in the public interest;
f) processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

Lawful Basis for Processing of Personal Data Policy

Individuals' Rights

5.4 The UK GDPR and the DPA gives individuals the following rights in regard to their personal data (and which is set out in the Data Protection Individuals' Rights Policy below):

5.4.1 Access their records;
5.4.2 Right to information;
5.4.3 Request that inaccurate data is rectified;
5.4.4 Request the erasure of records (right to be forgotten) or that the processing is restricted;(Please note that the right to the erasure of records or the restriction of processing is limited where the Council is required by law to process the personal data or where it is necessary for it to fulfill a public task);
5.4.5 Right not to be subject to automated decision-making;
5.4.6 Right to intervene in automated decision-making;
5.4.7 Right to information about decision-making;
5.4.8 Right to object to processing.

Data Protection Individuals' Rights Policy

5.5 The Council will process data in accordance with a data subject's legal rights as set out above.

5.6 The Council will ensure that any requests are handled courteously, promptly and fully in accordance with the UK GDPR and the DPA. The Council will take steps to ensure that either the data subject or his/her authorised representative has a legitimate case for exercising their right and that the request is valid and that information provided is clear and unambiguous.

6. Policy

Handling and Collecting Information

6.1 The Council will process all personal data for the purpose of providing an effective delivery of service in accordance with the aims, responsibilities and obligations of the Council.

6.2 The Council will maintain a record of its processing activities and review its processing to ensure that it is accurate and up to date. Heads of Service are responsible for informing the DPO of any new purposes for which personal data are processed in order to ensure that the Council's statement of processing is kept up to date.

6.3 The Council will, at the point of collection and as far as it is practicable, inform individuals of all purposes for which the Council will use their personal data. The Council maintains a more detailed Privacy Notice, which is reviewed and updated on a regular basis.

6.4 The Council carries out data-matching exercises to identify any anomalies or inconsistencies and also for the prevention and detection of fraud and when required by law to do so.

6.5 The Council reserves the right to disclose information under certain circumstances where allowed by law to do so.

6.6 The Council will consider each request for disclosure individually. Where a disclosure takes place, the Council will only disclose the minimum amount of information required.

Records Management

6.7 The Council will only collect personal data where there is a clear purpose for collecting and using the information.

6.8 The Council will not hold personal data for longer than it is reasonably required to do so.

6.9 All Managers and Staff will take steps to ensure that the personal data they hold is accurate and, where necessary, kept up to date.

6.10 Opinions recorded on a file must be carefully and professionally expressed.

6.11 The Council has in place a Document Retention and Destruction Policy.

Security

6.12 All Managers and staff are responsible for ensuring that personal data is held securely at all times.

6.13 Paper files and manual records containing personal data must be kept secure both within and outside Council premises.

6.14 Access to all Council systems will be password protected and only authorised personnel will have access.

6.15 When working off site, Council employees are responsible for ensuring that personal data is held securely.

6.16 Records will be safely and responsibly disposed of when they are no longer required. All reasonable steps will be taken to guarantee that any data processor that the Council uses (e.g. a contractor) has appropriate technical and organisational security measures in place to safeguard personal data.

6.17 Further information and details can be found in the Golden Rules for protecting personal and special category data.

6.18 All staff, volunteers and contractors will adhere to the Council's Information Governance Policy.

Transfer of Data

6.19 The DPA and the UK GDPR set out very strict rules concerning the transfer of personal data to Third Countries or International Organisations. Such a transfer should not take place in any circumstances without the express approval of the DPO who will be responsible for giving the necessary legal advice.

Complaints, Enforcement and Dealing with Breaches

6.20 Any complaint regarding data protection must be passed immediately to the DPO.

6.21 Any Council employee, volunteer or contractor who suspects that a breach of the DPA or the UK GDPR has, or will occur, must report it to the DPO immediately. If an actual or suspected breach of the data protection principles has occurred, Managers must follow the procedure for managing breaches on data security. The Procedure for Reporting Data Breaches provides further information.

6.22 There is a statutory requirement for the Council to notify a data protection breach to the ICO within 72 hours. Failure to do so may result in the Council being fined up to £8.7 million.

6.23 All Council staff and contractors are expected to co-operate in full with any investigation undertaken by the DPO or the ICO into an alleged breach of data protection.

Record of Processing

6.24 Data controllers are responsible for maintaining a record of the processing activities which they undertake. The Council will maintain its record of processing and regularly review it so as to ensure that its register entry is accurate and up to date.

6.25 Staff are responsible for informing the DPO of any new purposes for which personal data are processed in order to ensure that the Council's records are kept up to date.

7. The Information Commissioner's Office

7.1 The ICO's role is to uphold information rights in the public interest. The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information. This role is enhanced under the UK GDPR and the DPA.

7.2 The ICO may use criminal prosecution, non-criminal enforcement and audit, depending on the circumstances. The ICO also has the power to impose very significant fines on a data controller (see paragraphs 2.3 and 6.22 above).

7.3 Some of the options open to the ICO where there has been a more serious breach of the DPA and the UK GDPR include the ability to:

7.3.1 serve information notices, assessment notices and enforcement notices where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure that they comply with the law;

7.3.2 issue monetary penalty notices in circumstances where there has been a failure to comply with any of the three categories of notices referred to above.

Penalty notices require payment to the ICO of an amount specified in the notices.

7.3.3 prosecute those who commit criminal offences under the DPA. Examples of such offences are:

7.3.3.1 knowingly or recklessly making a false statement in response to an Information Notice;

7.3.3.2 altering or concealing information in circumstances where a request has been made in exercise of a data subject access right and the person making the request would have been entitled to receive information in response to it.

7.4 If the offences are proven, significant fines may be imposed against the Council by the Criminal Courts.

8. Data Protection Contacts

8.1 **Statutory Data Protection Officer, Hillingdon Council: Glen Egan**. Please see his contact details as set out in paragraph 3.3 above.

8.2 **Information Commissioner's Office** https://ico.org.uk/global/contact-us/ (Includes lists of email addresses) Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Tel: 0303 123 1113.

9. Review Process

9.1 This policy will be reviewed every two years.