OADBY & WIGSTON BOROUGH COUNCIL

DATA PROTECTION POLICY

Policy Version Number: 2.0
Policy Author: Data Protection Officer
Authorisation By: Senior Management Team
Date of Policy Review: 25 May 2020

Oadby & Wigston
BOROUGH COUNCIL

Contents

1.0 Introduction

Background

1.1 Oadby and Wigston Borough council (OWBC) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

1.2 Personal data at OWBC can include employees (present, past and prospective), service users, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

1.3 Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulations (GDPR).

1.4 The DPA and the GDPR requires OWBC to comply with the key Data Protection Principles (see Appendix 1 below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.5 The DPA and the GDPR gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly (see Appendix 3 below).

1.6 The lawful and correct treatment of person-identifiable information by OWBC is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. This policy will help OWBC ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection and the GDPR Principles

1.7 OWBC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also has a duty to comply with guidance issued by the Information Commissioners Office.

1.8 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Council. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

1.9 The aim of this policy is to outline how the OWBC meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The

obligations within this policy are principally based upon the requirements of the DPA and GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix 2 (below).

2.0 What Information is Covered?

2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

3.0 Policy Statement

3.1 This document defines the data protection policy for OWBC. It applies to all person-identifiable information obtained and processed by the organisation and its employees.

It sets out:

- The organisation's policy for the protection of all person-identifiable information that is processed
- The responsibilities (and best practice) for data protection
- The key principles of the DPA and the GDPR.

4.0 Principles

4.1 The objective of this policy is to ensure the protection of information OWBC keeps in accordance with relevant legislation, namely:

- **To ensure notification;**

Annually notify the Information Commissioner about the OWBC's use of person-identifiable information.

- **To ensure professionalism;**

  All information is obtained, held and processed in a professional manner in accordance with the provisions of the DPA and the GDPR.

- **To preserve security;**

  All information is obtained, held, disclosed and disposed of in a secure manner.

- **To ensure awareness;**

  Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

- **Data Subject access;**

  Prompt and informed responses to subject access requests.

4.2 The policy will be reviewed periodically by the OWBC Senior Management Team. Where review and update is necessary due to legislative changes this will be done immediately.

4.3 In accordance with the council's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

5.0 Scope of this Policy

5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis.

5.2 The procedures cover all person identifiable information, electronic or paper which may relate to employees, contractors and third parties about whom we hold information.

6.0 Policy

6.1 OWBC obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- Staff records and administrative records
- Service Users records including the administering of benefits, council tax, housing records, elections, grants, planning applications, licensing applications etc.
- Matters relating to the prevention, detection and investigation of offences , fraud and corruption
- Matters relating to the enforcement of primary and secondary legislation
- Complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data, OWBC will comply with the data protection principles within the DPA and GDPR.

7.0 Data Protection Responsibiliites

Overall responsibilities

7.1 The Council is the 'data controller' and permits the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Council has legal responsibility for the notification process and compliance with the DPA and the GDPR.

7.2 The Council whilst retaining its legal responsibilities has delegated data protection compliance to the Data Protection Officer.

Data Protection Officer's (DPO) responsibilities

7.4 The Data Protection Officer's responsibilities include:

- Ensuring that the policy is produced and kept up to date
- Ensuring that the appropriate practice and procedures are adopted and followed by the Council.

- Provide advice and support to the Senior Management Team on data protection issues within the organisation.

- Work collaboratively with Human Resources, the Head of Law and Governance and the Compliance Team to help set the standard of data protection training for staff.

- Ensure data protection notification with the Information Commissioner's Office is reviewed, maintained and renewed annually for all use of person identifiable information.

- Ensure compliance with individual rights, including subject access requests.

- Act as a central point of contact on data protection issues within the organisation.

- Implement an effective framework for the management of data protection.

Line managers' responsibilities

7.5 All line managers across the Council's service areas are directly responsible for:

- Ensuring their staff are made aware of this policy and any notices.

- Ensuring their staff are aware of their data protection responsibilities.

- Ensuring their staff receive suitable data protection training.

General responsibilities

7.6 All OWBC employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.7 All OWBC employees have a responsibility to inform their line manager and the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

7.8 All OWBC employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Compliance Officer.

7.9 Employees must follow the subject access request procedure (see Appendix 3 below).

8.0 Monitoring

8.1 Compliance with this policy will be monitored by the Finance and Corporate Governance team, together with internal audit reviews where necessary.

8.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

9.0 Validity of this Policy

9.1 This policy will be reviewed at least annually by the Senior Management Team. Associated data protection standards will be subject to an ongoing development and review programme.

Appendix 1: General Data Protection Regulation – The Data Protection Principles

1. Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy: Personal data shall be 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.

5. Storage Limitation: Personal data shall be 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 insofar 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 by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Integrity and Confidentiality: Personal data shall be 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.

7. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with, the previous six principles.

Appendix 2: Summary of Relevant Legislation and Guidance

General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. 'Controllers' and 'Processors' will be required to document decisions and maintain records of processing activities.

Human Rights Act 1998

This Act binds public authorities to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However, this article also states "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area. The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. OWBC issues each employee with an individual user id and password, which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act. OWBC will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its staff are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.

Appendix 3: Individual Rights of the Data Subject

1. The Right to be Informed: Individuals have the right to be provided with clear and concise information about what an organisation does with their personal data. OWBC has published Privacy Notices for each of its departments that outline in detail what data we collect, how that data is used, the lawful basis for processing the data and for how long we will retain that data. These can be found on our website at https://www.oadby-wigston.gov.uk/pages/privacy.

2. The Right of Access: Individuals have the right to access their personal data that is held by an organisation (commonly referred to as Subject Access). You have the right to obtain a copy of your personal data by making a Subject Access Request as detailed below.

3. The Right to Rectification: Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. You can make a request for rectification as detailed below.

4. The Right to Erasure: Individuals have the right to have their personal data erased or 'forgotten' in certain circumstances. These include when the data is no longer necessary for the purpose in which we originally collected or processed it, when we are relying on your consent to process the data and you choose to withdraw that consent, when we are relying on legitimate interests as our basis for processing and you object to this processing (so long as there is no overriding legitimate interest to continue this processing), we have processed the personal data unlawfully, we have to do it to comply with a legal obligation or we have processed the personal data to offer information society services to a child. The Right to Erasure is not an absolute right and only applies in these circumstances listed; however, we will make every effort to assist you. You can make a request for erasure as detailed below.

5. The Right to Restrict Processing: Individuals have the right to restrict or suppress the processing of their personal data where they have a particular reason for wanting the restriction. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the data, but not to use it. This right may apply if you are contesting the accuracy of your data and we are verifying that accuracy, if the data has been unlawfully processed and rather than invoking the Right to Erasure you request restriction instead, if we no longer need the personal data but you need OWBC to keep it in order to establish, exercise or defend a legal claim, or you object to our processing of your data and we are considering whether our legitimate grounds for processing override your request. You can request the restriction of data processing as detailed below.

6. The Right to Data Portability: Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. You have the right to request that we transfer the data you have provided to OWBC directly to another Data Controller. This right only applies when the lawful basis for processing the information is consent or for the performance of a contract and we are carrying out the processing by automated means (in other words, it excludes paper files). You can make a data portability request as detailed below.

7. The Right to Object: Individuals have the right to object to the processing of their data in certain circumstances. You have the absolute right to stop your data being used for direct marketing. You may also object to processing if it is for a task carried out in the public interest, the exercise of official authority vested in us or our legitimate interests (or those of a third party); however, the right to object is not absolute in these circumstances. You can make an objection as detailed below.

8. Rights in Relation to Automated Decision Making and Profiling: The GDPR has provisions on making a decision solely by automated means without any human involvement and the automated processing of personal data to evaluate certain things about an individual. All automated decision-making and profiling is subject to the GDPR and OWBC will identify, when applicable, whether any of our data processing relies solely on automated decision-making or whether we use profiling of any kind. This information is available on our website at https://www.oadby-wigston.gov.uk/pages/privacy.

To invoke these rights, simply submit your request to us in writing either by email at data.protection@oadby-wigston.gov.uk or to:

Oadby and Wigston Borough Council
Data Protection Officer
Council Offices
Station Road
Wigston
Leicestershire
LE18 2DR

For all requests, OWBC will have one calendar month in which to respond.