www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead
Data Protection Policy

December 2024

Contents

1 Introduction

The Royal Borough of Windsor and Maidenhead (RBWM) takes its obligations regarding compliance with the UK Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR) seriously. This policy sets out how RBWM manages those responsibilities.

RBWM processes personal data to operate and carry out its functions. Data subjects may include members of the public, all staff (prospective, current and past) employees, Councillors, clients, customers, suppliers and partner organisations. The processing of personal information is carried out in compliance with DPA 2018 and the GDPR.

RBWM regards the lawful and appropriate treatment of personal information as crucial to its successful operation and essential to maintaining confidence between the council and those whose personal data of which it is the custodian.

2 Definitions key terms

Processing:
means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR:
General Data Protection Regulation.

DPA:
Data Protection Act 2018.

DPIA
means a Data Protection Impact Assessment. This is a data protection risk assessment available on the intranet designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.

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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category personal data:
processing of 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 purpose of uniquely identifying a natural person,

data concerning health or data concerning a natural persona sex life or sexual orientation.

Data Subject:
means the identified or identifiable living individual to whom personal data relates.

3 Scope

This policy applies to all personal/special category personal data we process regardless of the location where that personal data is stored (e.g., on a laptop, pc or hard copy record).

The Corporate Leadership Team are responsible for ensuring all employees within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance.

All employees and others processing personal data on behalf of the council must read it. Failure to comply with this policy may result in disciplinary action.

4 Data Protection Principles

All personal data processing requires adherence to the following principles:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation).
3. The personal data processed is adequate, relevant and limited to what is necessary in relation to the purpose of processing (data minimisation).
4. Accurate and up to date (accuracy).
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purpose(s) for which the personal data is processed (storage limitation).
6. Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (security, integrity and confidentiality).

*See Appendix 1 for details on how to comply with all the above

principles.

5 Data Subjects Rights

- Be informed about the collection and the use of their personal data
- Access personal data (subject access requests (SARs)
- Have inaccurate personal data rectified
- Erasure (to be forgotten) in certain circumstances
- Restrict processing in certain circumstances

- Data portability
- Right to object to processing in certain circumstances
- Rights in relation to automated decision making and profiling
- Right to withdraw consent at any time (where relevant)
- Right to complain to the Information Commissioner (https://ico.org.uk/make-a-complaint/)

6 Data Protection Officer

RBWM has an appointed Data Protection Officer should you have any data protection concerns or queries. The DPO also acts as the single point of contact for the Information Commissioner's Office (ICO) and provides advice and assistance on DPIAs.

Data Protection Officer
Town Hall,
St Ives Road,
Maidenhead,
SL6 1RF
Email: DPO@rbwm.gov.uk

Appendix 1.

Principle 1. Lawfulness and fairness

You may only process personal data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing but ensure that you process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. The lawful basis for our processing can be found on the privacy notices published for each purpose of processing we do on our RBWM website.

RBWM are required to show the information journey for the personal data processed. We do this through our privacy notices. Our privacy notices are written to be concise, transparent, intelligible, in clear and plain language and easily accessible so that the data subject can easily understand the information journey their personal data takes for each purpose of processing.
Prior to the collection of personal data RBWM must provide or signpost the data subject to a privacy notice, setting out the following:

1. The name of the service processing the personal data.

2. The lawful basis of the processing.

3. What categories of personal data is collected.

4. The purpose of the processing.

5. Who has access to the personal data.

6. Who we may share the personal data with.

7. How long we store the personal data.

The data subject must be provided with all the information required by the GDPR prior to the processing or as soon as possible after collecting/receiving the data. We must also check that any personal data collected by a third party was done so in accordance with the GDPR and DPA 2018.

2. Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

1. You cannot therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes. Where the further processing is not based on the data subject's consent or on a lawful exemption from data-protection law requirements, you should assess whether a purpose is incompatible by taking into account factors such as the:

1. Link between the original purpose/s for which the personal data was collected and the intended further processing. Context in which the personal data has been collected – would the data subject reasonably anticipate the further processing of his/her personal data.

2. Nature of the personal data in particular whether it involves special categories of personal data or personal data relating to criminal offences/convictions.

3. Consequences of the intended further processing for the data subjects.

4. Existence of any appropriate safeguards e.g. encryption or pseudonymisation.

Principle 3. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You should not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that you can fulfil the purposes for which it was intended to be processed.

You may only process personal data when performing job duties that requires it and you should not process personal data for any reason unrelated to the job duties, to do say may result in dismissal and even police action.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with your privacy notice specified data retention period.

Principle 4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. You should ensure that personal data is recorded in the correct files.

Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, you should ensure that relevant records are completed.

You must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should up-date, out-of-date personal data where necessary (e.g. where it is not simply a pure historical record).

Where a data subject has required his/her personal data to be rectified or erased, you should inform all other recipients you have shared the personal data with of the request, unless it is impossible or significantly onerous to do so.

Principle 5. Storage limitation

You must not keep personal data in a form that allows data subjects to be identified for longer than needed for the purposes for which it was collected. Those purposes include satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from RBWM systems all personal data that we no longer require in accordance with all relevant records retention schedules and policies.

You will ensure that data subjects are informed of the period for which their personal data is stored or how that period is determined in any relevant Privacy Notice.

Principle 6. Security, Integrity and Confidentiality

RBWM is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data. You should consider whether a DPIA is necessary. Safeguarding will include the use of encryption and pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

You are responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting special category personal data from loss and unauthorised access, use or disclosure.

You must comply with all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

You must comply with all applicable aspects of our Information Security Policy and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Law standards to protect personal data.

You may only transfer personal data to third-party service providers (e.g. data processors) if they provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Law and who agree to act only on RBWM instructions. All third parties who process personal data on behalf of RBWM should have either a contract with the full GDPR contract clauses and/or an up to date Information Sharing Agreement (ISA). Guidance on producing or signing an ISA should be sought from the Data Protection Officer dpo@rbwm.gov.uk

Any data protection breach or concern should be reported immediately here:

RBWM personal data breach or concern reporting form | Data Protection and privacy notices – The Royal Borough of Windsor & Maidenhead

Document Name	RBWM Data Protection Policy		
Document Author	Samantha-Lea Wootton, RBWM Data Protection Officer		
Document owner	Samantha-Lea Wootton		
Accessibility			
File location	Y drive, PR, RFIR, Data Protection/GDPR, Data Protection Policy		
Version control	Version 1		
	Version 2		
	Version 3		
Next review date	December 2025		