TONBRIDGE & MALLING BOROUGH COUNCIL

www.tmbc.gov.uk

# Data Protection Policy



DECEMBER 2024

# 1 Introduction

## Introduction

1. The Council is required under the UK GDPR & Data Protection Act 2018 to ensure the security of all personal data it processes including that processed by third parties acting on its behalf. We need to collect and use certain types of information about people with whom we deal in order to deliver our services.

2. One of the four priorities within the Council's Corporate Strategy 2023-2027 is to provide "Efficient services for all residents, maintaining an effective Council." This policy will contribute to the delivery of this strategic priority by ensuring we handle personal information securely and efficiently.

3. This policy applies to all personal data processed by the Council.

4. The UK GDPR defines personal data as "any information relating to an identified or identifiable natural person (data subject). Examples of personal data include:-

   - Personal information, such as name and address.
   - Family details.
   - Lifestyle and hobbies.
   - Education and training.
   - Health-related information.
   - Employment data.
   - Financial information.

5. Examples of special category personal data include:-
   - Racial or ethnic origin.
   - Political opinions.
   - Religious and philosophical beliefs.
   - Trade union membership.
   - Genetic data.
   - Biometric data for the purpose of uniquely identifying a natural person.
   - Data concerning health.
   - Sex life and sexual orientation.

## Legislative framework – the Data Protection Principles

6. There are seven Data Protection Principles contained in the UK GDPR which must be complied with when processing personal data. Failure to comply with any of these Principles is a breach of the UK GDPR.

   Personal information should be:-

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

   2. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

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

   4. 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');

   5. 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

   6. 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 data controller shall be responsible for and be able to demonstrate compliance with the above (the 'accountability' principle). This is explained in more detail at paragraph 7 below.

## Accountability Principle

7. We must be able to demonstrate compliance with the above Principles. Our Data Protection Officer is responsible for monitoring our compliance with these Principles. We will:
   - ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request;
   - carry out a Data Protection Impact Assessment for any high-risk personal data processing, and consult the Information Commissioner if appropriate;
   - ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the Council's personal data handling and that this person has access to Management Team;
   - have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection legislation.

## Corporate Privacy Notices

8. The council collects and uses personal information for a number of purposes across all of its departments and functions. Privacy notices for each service may be viewed on the Council's website at https://www.tmbc.gov.uk/privacy-notice.

## Data Retention

9. We cannot keep data for longer than we need it. The Data Protection Act/ UK GDPR does not set specific time limits for retention of different types of data. Unless there are legal or regulatory requirements to retain data for a specific period, it is up to us to determine our retention periods, which will depend on how long we need the data for our specified purposes.

10. Our Data Retention Policy sets out the time periods we will adhere to for the retention of personal data. These will also be explained in the relevant privacy notice.

11. Our Data Retention Policies may be viewed on our website at TMBC privacy notices by service – Tonbridge and Malling Borough Council.

## Data Subject Rights

12. You have certain rights in respect of your personal data. These guidelines provide a framework for responding to requests to exercise those rights in accordance

with Data Protection legislation. Your rights are set out below.

- Right to access your personal information - known as subject access requests (SARs)
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

13. Where a request to exercise a right is made, we will, unless an exemption applies, comply with your request without undue delay and usually within one calendar month of the date of receipt of your request. If the request is complex, or there are a number of requests, we may extend the period for responding by up to two additional calendar months. If we extend the period for responding, we will inform you within one month of receipt of the request and explain the reason for the delay.

14. We may refuse to deal with a request where we consider it is manifestly unfounded or excessive or alternatively we may charge a 'reasonable fee' to deal with the request. If we are not going to respond to your request for rectification, we will inform you of the reason(s) for not taking action and of your right to make a complaint to the ICO/ seek a judicial remedy.

## How to access your rights

## (1) Subject Access Requests (SARs)

15. You have the right to find out what information we hold about you.

16. We do not have to comply with a SAR, if doing so means disclosing information which identifies another individual, except where:
    - the other individual has consented to the disclosure; or
    - it is reasonable to comply with the request without that individual's consent.

17. **How can you find out what information is held about you? -** You may make your request either verbally or in writing e.g., by letter, e-mail or online. Someone else can make a request on your behalf only if we are satisfied that they have your permission to do so.

18. **Is a fee payable?** - In most cases, we cannot charge a fee to comply with a SAR. However, we can charge a 'reasonable fee' for the administrative costs of complying with a request if:
    - it is manifestly unfounded or excessive; or
    - you request additional copies.

19. Alternatively, we can refuse to comply with a manifestly unfounded or excessive request.

20. When determining a reasonable fee, we can take into account the administrative costs of:
    - assessing whether or not we are processing the information; locating, retrieving and extracting the information; providing a copy of the information; and
    - communicating the response to you, including contacting you to inform you that we hold the requested information (even if we are not providing the information)

21. A reasonable fee may include the costs of photocopying, printing, postage and any other costs involved in transferring the information to you (e.g. the costs of making the information available remotely on an online platform); equipment and supplies (eg discs, envelopes or USB devices); and staff time. We will base the costs of our staff time on the estimated time it will take staff to comply with the specific request, charged at a reasonable hourly rate.

22. We will not respond to a subject access request until we have confirmed your identity and address.

23. We will not respond to a subject access request until you have paid your fee, where applicable.

## (2) Request to rectify personal data ('right to rectification')

24. Personal information is inaccurate if it is incorrect or misleading as to any matter of fact. You have the right to have your inaccurate personal information rectified or completed if it is incomplete.

## (3) Request to erase personal data ('right to be forgotten')

25. The right to erasure is not absolute and only applies in certain circumstances. For example, we can refuse to deal with a request for erasure where we are under a legal obligation to process your personal information in order to perform a task in the public interest.

26. You have the right to have personal information erased and to prevent processing in specific circumstances:

- where retention of the personal data is no longer necessary in relation to the purpose for which it was originally collected.
- you have withdrawn your consent to the processing of your personal data and no other legal justification for processing applies.
- You have objected to processing that is either:-
    - Necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council;
    - Necessary to pursue a legitimate interest; and
    - No other compelling legitimate grounds for processing apply.
- the personal information was unlawfully processed (i.e., otherwise in breach of the GDPR).
- the personal information has to be erased in order to comply with a legal obligation.
- You object to the processing of your personal data for direct marketing purposes.

27. The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future.

## (4) Request to restrict processing of personal data

28. The right to restrict processing is not absolute and only applies in certain circumstances.

29. You have the right to restrict processing of your personal information in circumstances set out below:

- you contest the accuracy of your personal information - we will restrict the processing until we have verified the accuracy of the personal information.
- you have objected to the processing that relies upon the public interest or a third party's legitimate interests as the lawful basis for processing – we will restrict the processing whilst we are considering whether our/ the third party's legitimate grounds override yours.

- the processing is unlawful. Instead of requesting erasure, you may request that the Council restricts use of the unlawfully processed personal data.
- if we no longer need your personal information but you require the personal information to establish, exercise or defend a legal claim.

## (5) Data portability

30. You have the right to obtain from us and reuse your personal information for your own purposes across different services. This right only applies to information you have supplied to us and in the following circumstances:-
    - The lawful basis relied upon by the Council for processing the information is consent or for the performance of a contract
    - We are carrying out the processing by automated means i.e. excluding paper files.

31. Where this right applies you are entitled to receive a copy of your personal information in a structured, commonly used and machine readable form and/ or have your personal data transmitted to another data controller.

32. We will consider the technical feasibility of a transmission on a request by request basis. The right to data portability does not create an obligation for us to adopt or maintain processing systems which are technically compatible with other systems.

## (6) Objecting to the processing of personal data

33. You have a right to object to
    - processing based on the performance of a task in the public interest/legitimate interests (including profiling);
    - direct marketing (including profiling); and
    - processing for purposes of scientific/historical research and statistics, unless the processing is necessary for the performance of a task carried out in the public interest.

34. Where the objection is to processing your personal information for direct marketing purposes, we must stop processing your personal information when we receive your objection.

35. Where the objection is to processing your personal information for the performance of a public interest task or legitimate interests we must stop processing your personal information unless we can demonstrate compelling

legitimate grounds for the processing which override your interests, or, the processing is for the establishment, exercise or defence of legal claims.

## (7) Automated decision making and profiling

36. You have the right not to be subject to solely automated decision-making, including profiling, which has legal or other similarly significant effects on you.

37. This right does not apply when the automated decision is:-
- Necessary for entering into or performing a contract with you;
- Required or authorised by domestic law which requires suitable measures to safeguard your rights and freedoms and legitimate interests;
- Based upon your explicit consent

## Key Contacts

38. The Council's appointed Data Protection Officer is Adrian Stanfield, Director of Central Services and Deputy Chief Executive.

39. The Council's appointed Senior Information Risk Owner (SIRO) is Ganesh Thanagarajah, Head of IT.