City of Bradford Metropolitan District Council

Policy on Handling
Data Subject Requests (GDPR)

1. Purpose

The City of Bradford Metropolitan District Council ("The Council") has adopted this policy to address procedures for handling data subject requests and objections under the General Data Protection Regulation (GDPR) when the Council acts as a data controller.

The GDPR grants data subjects certain rights regarding their personal data including the right:

- To access their personal data (GDPR Article 15).
- To correct their personal data (GDPR Article 16).
- To erase their personal data (GDPR Article 17).
- To restrict personal data processing about them (GDPR Article 18).
- To receive a copy of certain personal data or transfer that personal data to another data controller, also known as the data portability right, (GDPR Article 20).
- To object to personal data processing (GDPR Article 21).
- Not be subject to automated decision-making in certain circumstances (GDPR Article 22).

This policy formalises the Council procedures for:

- **Confirming** the identity of the data subject making a request, or the identity, and legal authority, of the third party making a request, on a data subject's behalf.
- **Recording and tracking** data subject requests and responses, including all correspondence and internal documents related to requests.
- **Identifying and locating** relevant personal data.
- **Determining** whether a GDPR or Data Protection Act 2018 exemption exists that permits or requires the Council to refuse to fulfil the request.
- **Handling** data subject requests that involve several data subjects' personal data.
- **Communicating** with data subjects at reasonable intervals regarding the status of their request.

2. Scope

This Policy applies to all Council employees, including Council members, contractors, partner organisations and data processors acting on behalf of the Council. Detailed guidance on how this policy will be implemented is available.

3. Data Subject Request Submission Format

The Council requires that all data subjects, seeking to exercise their GDPR rights use the Council's standard request forms. These forms ask data subjects for specific information necessary to process and respond to their request.

Data subjects must submit the form applicable to their type of request which can be found on the Council's website make-a-data-protection-request.

If a data subject cannot access or fill out the online form, they can submit their requests, detailing which of the GDPR rights they are exercising,

- via email to DPO@bradford.gov.uk
- via the postal service addressed to the Corporate Information Governance Team, City of Bradford Metropolitan District Council, City Hall, Centenary Square, Bradford, BD1 1HY
- via telephone - 01274 434506

4. Tracking Data Subject Requests

The Council will ensure that all data subject requests received are forwarded, in the first instance, to the Corporate Information Governance Team where the full details of the request will be logged, a responding Council Service or Department assigned and progress tracked until the request is concluded.

5. Acknowledging Receipt of Data Subject Requests

The Council will acknowledge receipt of all requests and provide the time frame within which the data subject should expect to receive a response. For online requests and email requests to dpo@bradford.gov.uk this will be by automated response.

6. Proof of Data Subject's Identity

Where appropriate the Council will verify a data subject's identity before responding to a data subject request and will ask for identification that clearly shows their name, date of birth, and current address. The one-month time frame to respond to a data subject request does not start until the Council receive a fully completed request and proof of identity.

The Council will accept a photocopy, scanned image or photograph of a passport or other identification such as a driver's license, national identification number card, or birth or adoption certification as proof

of name and date of birth.

For proof of address the Council will accept a utility bill, bank statement or other official document.

If the data subject has changed their name, the Council will require that they provide relevant documents evidencing the change.

Where the data subject is a Council employee then normally proof of identity will not be required, particularly in cases where the data subject opts for their requested information to be sent to their workplace email address. However, where this does not happen and the data subject identity is in doubt then further proof may be requested.

Where the Council cannot verify the data subject's identity based on the information provided, or if the data subject has not included all the required forms of identification the Council will advise the data subject in writing (via email or post) that additional information is required.

A third party may make a request on a data subject's behalf. In this case, the Council require proof of the data subject as shown above **and** third party identity as shown above **and** evidence of the third party's legal right to act on the data subject's behalf.

The Council will accept a copy of the following as proof of the third party's legal authority to act on the data subject's behalf:

- a written consent signed by the data subject,
- a certified copy of a power of attorney or evidence of parental responsibility

The Council will not normally store identification documentation provided by data subjects or a 3rd party on their behalf for longer than 24 hours, before it is destroyed. However where the Council requires storing this for longer the Council will only use the documentation to respond to the data subject request and not for any other purpose.

7. Identifying and Locating Relevant Personal Data

The Council will ensure that the Service / Department to whom the request is assigned will locate the personal data relevant to the data subject request.

Where the scope of the data subject request is unclear or does not provide sufficient information to conduct a search then the Council will request that the data subject provide more specific information to process the request and locate the relevant personal data.

8. Time to Respond to Data Subject Requests

The Council will respond to data subject requests no later than one month after receiving the request unless an exception applies.

If the Council determines that a data subject request may take longer than one month to respond to then it will consider extending the one-month response time and notifying the data subject explaining the reasons for the delay.

9. General Reasons for Denying a Data Subject Request

The Council will, on occasion, determine if there is a basis not to respond to a data subject request. The Council will normally refuse to respond to data subject requests for the following reasons:

- A third party fails to present sufficient proof of authority to make the request on the data subject's behalf.
- Where the Council processes data for purposes that do not require data subject identification and the Council demonstrates that it cannot identify the data subject, it may deny data subject requests under Articles 15 (right of access), 16 (right to rectification), 17 (right to erasure), 18 (right to restrict processing), and 20 (right to data portability) unless the data subject provides additional information enabling identification.

- The Data Protection Act 2018 provides a basis for denying the request.

- The Council demonstrates that the request is manifestly unfounded or excessive, in particular because of its repetitive character.

- The Council does not hold any personal data related to the data subject request.

Please note that these general grounds are in addition to the specific grounds for denying a request made under Articles 15 (right to access), 16 (right to rectification), 17 (right to erasure), 18 (right to restrict processing), 21 (right to object to processing), and 22 (automated processing exception) which are described in Paragraphs 11 through 17 of this policy.

Where the Council refuses to respond to a data subject request the Council will explain the refusal to data subjects, without undue delay, and at the latest within one month after receipt of the request (unless a determination is made to extend the response deadline). The Council will advise the data subject of their right to complain to the Information Commissioner.

If, following a diligent search for records related to the data subject's request the Council do not have or process personal data related to the data subject, the data subjects will be informed in writing.

10. Fees for Responding to Data Subject Requests

The Council will normally respond to a data subject request without charge, however, fees may be charged where requests are manifestly unfounded or excessive, because of their repetitive character or when the request relates to large amounts of data or where a data subject requests additional copies of their data.

The Council will determine on a case by case basis whether a fee will be charged, the amount and the reasons for charging the fee and advise data subjects accordingly.

11. Responding to Subject Access Requests (SAR's)

Data subjects have the right to request access to their personal data processed by the Council under Article 15 of the GDPR and in response to a data subject access request the Council will, unless an exemption applies, provide data subjects with the information about its personal data processing activities.

The Council will, unless an exemption applies, provide the data subject with a copy of the personal data the Council process, about the data subject, in a commonly used electronic form.

In certain cases, the Council will process personal data that contains the personal data of several data subjects and in these cases the Council will ensure that the data subject access right does not adversely affect the rights and freedoms of third parties.

Where the data set includes third parties' personal data, the Council will determine whether there is a legal basis to release the third parties' data. Where no legal basis to release is identified then the Council will redact or remove the personal data of the third parties prior to providing the data in response to an access request.

In addition to the general grounds for denying a data subject access request, set out in paragraph 9, the Council may also refuse to respond to a data subject request if the data subject requests a copy of the personal data the Council processes and the provision of this is likely to adversely affect the rights and freedoms of others.

12. Responding to Correction (Rectification) Requests

Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data.

Where a rectification request is made, the Council will rectify the personal data without undue delay unless a basis exists to deny such a request. Where this happens the Council will inform the data subject of the reason(s) for not acting and of the possibility of lodging a complaint with the Information Commissioner.

13. Responding to Erasure Requests

Data subjects have the right, in certain circumstances, to request that the Council erase their personal data. Where such a request is made, unless an exemption applies, the Council will erase the personal data that is the subject of the request.

Where the Council determines that it must erase the data subject's data in response to the request, and the Council made the personal data that is the subject of the erasure request public, reasonable steps, including technical measures, will be taken to inform other organizations processing the personal data of the erasure request, including removing any links to, and copies of, the personal data.

Where the Council determines that it must erase the data subject's data in response to the request, each recipient, to whom the Council disclosed the personal data that is the subject of the erasure request, will be identified and the decision to erase the personal data will be communicated to the third-party data recipients, unless the Council finds that this is impossible or involves disproportionate effort.

In addition to the general grounds for denying a data subject request set out in section 9 above, the Council may also refuse to respond to a data subject erasure request if the Council processes personal data that is necessary for:

- Exercising the right of freedom of expression and information.
- Complying with a legal obligation under UK or EU law.
- The performance of a task carried out in the public interest.
- Exercising the Council's official authority.
- Public health reasons consistent with the exceptions for processing sensitive personal data such as health information, as outlined in GDPR Articles 9(2)(h) and (i) and 9(3).
- Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes under Article 89(1), if the erasure is likely to render impossible or seriously impair the processing objectives.
- The establishment, exercise, or defence of legal claims.

Where the Council determines that there is a basis not to respond to a data subject erasure request, the data subject will be advised of the reason(s) for not acting and of the possibility of lodging a complaint with the Information Commissioner.

14. Responding to Requests to Restrict Personal Data Processing

Data subjects have the right, in certain circumstances, to request that the Council restrict the processing of their personal data. Where such a request is made, the Council will, unless an exemption applies, restrict processing of the data subject's personal data.

Where the Council has a legal basis for not responding to the data processing restriction request the data subject will be informed of the reasons for not acting and of the possibility of lodging a complaint

with the Information Commissioner.

15. Responding to Data Portability Requests

Data subjects have the right, in certain circumstances, to receive a copy of certain personal data from the Council in a structured, commonly used, and machine-readable format and store it for further personal use on a private device; transmit certain personal data to another data controller; ask the Council to transmit certain personal data directly to another data controller, where technically possible.

The Council will only supply personal data concerning the data subject which the data subject knowingly and actively provided to the Council, e.g. name, contact information, and browsing history. The Council will not, however, provide data that is created from the data provided by the data subject e.g. a user profile.

Where the data set includes third parties' personal data the Council will transfer the third parties' data where there is a legal basis to do so.

In addition to the general grounds for denying a data subject request set out in section 9, the Council may also refuse to respond to a data subject portability request if responding to the request adversely affects the rights and freedoms of others.

Where the Council has a basis not to respond to a data portability request, the data subject will be informed of the reason(s) for not acting and of the possibility of lodging a complaint with the Information Commissioner.

16. Responding to Objections to Personal Data Processing

Data subjects have the right to object to personal data processing when the Council processes their personal data for direct marketing purposes (including profiling related to direct marketing), scientific or historical research purposes, statistical purposes, processing for a task carried out in the public interest or the exercise of official authority or processing necessary for the legitimate interests of the Council or a third party.

The Council will stop the personal data processing related to the data subject's request unless an exemption applies or the Council can demonstrate that the processing is necessary for it to perform a task in the public interest or there is a compelling legitimate ground for processing the personal data that overrides the data subject's interests or where there is a need to process the personal data to establish, exercise, or defend legal claims.

Where the Council has a basis not to respond to a data subject objection request, the data subject will be informed of the reason(s) for not acting and of the possibility of lodging a complaint with the Information Commissioner.

17. Responding to Automated Decision-Making Objections

Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, including profiling, if the decision produces legal or other similarly significant effects on them.

The Council will determine if the automated decision-making, including profiling, produces legal effects on the data subject or affects them in a similarly significant way and will, unless an exemption applies, stop the automated decision-making that is the subject of the data subject request.

In addition to the general grounds for denying a data subject request set out in section 9, the Council will refuse to grant an automated decision-making objection when the automated decision is either necessary for entering into or performing a contract with the data subject; authorised by an EU or member state law applicable to the Council; based on the data subject's explicit consent.

Where the Council has a basis not to respond to the data subject's automated decision-making objection, the data subject will be informed of the reason(s) for not acting and of the possibility of lodging a complaint with the Information Commissioner.

18. Training and Awareness

The Council will publish this policy, on both internal and external websites, and ensure that all appropriate staff understand their roles in implementing this policy.

19. Enforcement

Violations of or actions contrary to this policy may result in disciplinary action, in accordance with the Council's Human Resources policies.