Three Rivers District Council

Subject Access Request Policy

2025 - 2028

THREE RIVERS DISTRICT COUNCIL

Contents

1. Introduction

Three Rivers District Council (the Council) is committed to protecting the privacy rights of individuals in accordance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR), together referred to as the Data Protection Legislation. This policy outlines the procedures for handling Subject Access Requests (SARs) to ensure compliance with the Data Protection Legislation while ensuring transparency and upholding the rights of individuals regarding their Personal Data.

2. Scope

This policy applies to all employees, councillors, volunteers, contractors, and agents working for or on behalf of the Council who process Personal Data as part of their roles. It covers all Personal Data processed by the Council, regardless of the format in which it is held. This policy only applies when the Council acts as the Data Controller and not when the Council acts as the Data Processor.

3. Definitions

Data Controller: The entity that determines the purposes and means of processing Personal Data.

Data Processor: The entity that processes Personal Data on behalf of the Data Controller.

Data Subject: The identified or identifiable natural person to whom the Personal Data collected and processed by the Council relates.

Personal Data: Any information relating to an identified or identifiable Data Subject.

Subject Access Request: A request made by a Data Subject to access their Personal Data held by the Council.

4. Legal Basis

Under the UK GDPR, Data Subjects have the right to access their Personal Data held by the Council. This policy ensures that the Council meets its legal obligations by providing a structured approach to handling Subject Access Requests.

5. Rights of the Data Subject

Under UK GDPR, Data Subjects have the right to:

- Know if their Personal Data is being processed.
- Access their Personal Data.
- Be informed of the purposes of the processing, the categories of Personal Data concerned, and the recipients of the Personal Data.
- Request correction or erasure of their Personal Data.
- Restrict processing of their Personal Data.
- Receive a copy of certain Personal Data or transfer that Personal Data to another Data Controller.
- Object to Personal Data processing.

6. Making a Subject Access Request

Subject Access Requests can be submitted via our online portal, in writing, via email, via social media or verbally. Upon receipt, requests will be directed to the Data Protection Officer (DPO).

Requests should include:

- The Data Subject's full name and contact details.
- Any information that will assist in locating the requested Personal Data (e.g.,

specific departments, relevant time periods).

7. Identification and Verification

To ensure the protection of Personal Data, the Council will verify the identity of the requester before processing a Subject Access Request. Acceptable forms of identification include:

- Passport.
- Driver's License.
- Utility Bill (dated within the last three months).
- Birth Certificate.
- Any other form of identification deemed appropriate by the Data Protection Officer.

If the requester is acting on behalf of the Data Subject, the Council will also require written authorisation from the Data Subject and proof of the requester's identity.

8. Handling a Subject Access Request

Upon receipt of a Subject Access Request, the following steps will be taken:
Acknowledge Receipt: The Council will acknowledge the request within 3 working days, confirming receipt and outlining the next steps.

Verify Identity: The Council will verify the identity of the requester. If the identity cannot be verified, the Council will request additional identification.

Clarify Request (if necessary): If the request is ambiguous or too broad, the Council will contact the requester for clarification. The processing period may be paused until clarification is received.

Data Retrieval: The DPO will coordinate with relevant departments to retrieve the requested Personal Data. All efforts will be made to locate and collate the Personal Data fully and accurately.

Review Data: The DPO will review the Personal Data to ensure it does not include information on third parties or information that is exempt from disclosure, redacting or not supplying information as appropriate. Where redactions are made, the Council will ensure that these cannot be technically undone and that there is not hidden data, for example in spreadsheets.

Respond: The Council will provide the information in a concise, transparent, and easily accessible form within one calendar month of receipt of the request. If the request is complex, an extension of up to two additional months may be applied, with notification to the requester.

9. Format of Responses

The Council will provide the information in the format requested by the Data Subject, if possible. This may include:

- Electronic copies (e.g, PDF).
- Printed copies.
- On-screen inspection at the Council offices.

10. Exemptions

The Council may refuse to comply with a Subject Access Request if it is manifestly unfounded, excessive, or if an exemption applies. The Data Subject will be informed of the reason for refusal and their right to complain to the Information Commissioner's Office (ICO). Contact details for the ICO can be found below.
Certain Personal Data is exempt from disclosure under the UK GDPR and the Data Protection Act 2018. Exemptions may include, but are not limited to:

- Information that identifies third parties without their consent.
- Data related to crime prevention and investigation if disclosure who prejudice the prevention or detection of crime.
- Confidential references given or received by the Council.
- Information subject to legal professional privilege.
- Data processed for research, historical, or statistical purposes where it would prevent or seriously impair the achievement of the purposes.

11. Fees

In most cases, the Council will not charge a fee to respond to Subject Access Requests. This policy ensures that individuals can exercise their rights to access Personal Data without financial barriers. However, if a request is found to be manifestly unfounded or excessive—often due to being repetitive or requiring a disproportionate amount of time or resources—the Council may impose a reasonable fee rather than reject the request. This fee will be calculated based on actual administrative costs incurred in processing the request, ensuring transparency in the calculation.

The Council will provide a breakdown of any fees, detailing the staff time and material costs involved. Prior to proceeding with the request, the requester will be informed of these fees, allowing them to make an informed decision about whether to continue. Payment procedures will be clearly outlined, including accepted payment methods and any timelines for payment. Importantly, requesters have the right to appeal any fee decisions if they believe the charges are unjustified or excessive, providing an additional layer of fairness in the process.

12. Record Keeping

The Council will maintain a detailed record of all Subject Access Requests received, including:

- Name of applicant.
- Date of receipt.
- Date of acknowledgment.
- Date of response.
- Nature of the data provided.
- Any communications with the requester.
- Any exemptions applied.
- Time taken to fulfil.

These records will be kept securely and in compliance with UK GDPR principles.

13. Data Subject Rights

In addition to the right to access their Personal Data, Data Subjects have other rights under UK GDPR, including:

- The right to rectification.
- The right to erasure (right to be forgotten).
- The right to restrict processing.
- The right to data portability.
- The right to object to processing.
- Rights in relation to automated decision making and profiling.

The Council will provide information on how Data Subjects can exercise these rights in our privacy notices.

14. Data Security

The Council is committed to ensuring the security of Personal Data. All staff are trained on data protection principles and the importance of data security. This is recertified bi-annually.

Appropriate technical and organisational measures are in place to protect Personal Data from unauthorised access, alteration, disclosure, or destruction.

15. Training and Awareness
All employees involved in the collation of Subject Access Requests will be trained to do so, with guidance and final oversight coming from the DPO.

16. Complaints
If a Data Subject is not satisfied with the response to their Subject Access Requests, they have the right to make a complaint via the Councils Corporate Compliments & Complaints Policy.

The complaint will be reviewed by a senior member of staff who was not involved in the original decision. The Council will aim to reply to the complaint within 20 working days. If the Data Subject remains unsatisfied, they have the right to lodge a complaint with the UK data protection regulator, the Information Commissioner's Office (ICO).

Contact Information for ICO:
Email: icocasework@ico.org.uk
Telephone: 0303 123 1113
Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Website: https://ico.org.uk/

17. Monitoring and Review
This policy will be formally reviewed every three years or when there are significant changes in the law or Council procedures.
The Council will monitor compliance with this policy and the effectiveness of its procedures for handling Subject Access Requests.

DOCUMENT INFORMATION

	Name	Position	Date
Prepared by:	Jamie Russell	Resilience and Risk Officer	May 2025
Checked & Reviewed by:	Phil King	DP and Resilience Manager	May 2025
Approved by:	CMT	Corporate Management Team	10/06/2025
	P&R Committee	Policy and Resources Committee	21/07/2025
Next review date:	December 2027		
Version:	1.0		
Reason for document issue:	New policy following review of all data management policies		

Distribution List

Quantity & Format	Name	Position	Date
1 x electronic	Website		22/07/2025

Amendment & Revision Record

Version Number	Purpose of issue	Date
1.0	New policy following review of all data management policies	22/07/2025

THREE RIVERS
DISTRICT COUNCIL