Three Rivers District Council

Special Category Personal Data and Criminal Offence Data Policy

2025 - 2028

THREE RIVERS DISTRICT COUNCIL

1. Introduction

This policy outlines Three Rivers District Council's approach to the handling, processing, storage, and safeguarding of Special Category Personal Data and Criminal Offence Data. These types of data are considered more sensitive, and as such, require enhanced protection measures in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The Council is committed to upholding the principles of data protection and ensuring the confidentiality, integrity, and security of all personal data under its control.

2. Scope

This policy applies to all employees, departments, elected Members, third-party contractors, and any external partners engaged by the Council who have access to or handle Special Category Personal Data or Criminal Offence Data on behalf of the Council. This includes data collected directly from individuals, as well as data received from third parties or generated as part of the Council's operational activities.

This policy also applies to digital, physical, and paper records containing Special Category Personal Data and Criminal Offence Data.

3. Definitions

Special Category Personal Data: Personal data that is more sensitive and requires additional protection. This includes, but is not limited to, data concerning

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- health data
- data concerning a person's sex life or sexual orientation.

Criminal Offence Data: Data related to the commission or alleged commission of criminal offenses, including convictions and related security measures.

4. Legal Basis for Processing

Under the UK GDPR, the processing of Special Category Personal Data and Criminal Offence Data must have a lawful basis. The Council will only process such data where:
Special Category Personal Data: Processing is necessary for the performance of obligations in employment, social security, or social protection law; protection of vital interests; consent; or other legitimate public interest purposes, as specified in Article 9 of the UK GDPR.

Criminal Offence Data: Processing is necessary for carrying out obligations under UK law, including the prevention or investigation of crime, as detailed in Article 10 of the UK GDPR and the Data Protection Act 2018.

5. Data Security and Confidentiality

The Council is committed to ensuring that Special Category Personal Data and Criminal Offence Data are processed securely to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage. Appropriate technical and organisational measures will be implemented to ensure data security, including:

- Encryption
- Access controls
- Regular data audits
- Data pseudonymisation and anonymisation (where appropriate)

Access to Special Category Personal Data and Criminal Offence Data will be restricted to authorised personnel who require access in the course of their duties.

6. Data Retention

Special Category Personal Data and Criminal Offence Data will only be retained for as long as necessary to fulfil the purpose for which it was collected and in accordance with the Council's retention schedule. Once this period has elapsed, the data will be securely disposed of, in line with the Councils Data Retention Policy.

7. Data Subject Rights

Individuals have specific rights under the UK GDPR regarding their personal data, including:

- Right to access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object to processing

In cases involving Special Category Personal Data and Criminal Offence Data, the Council may not be able to comply with some rights (e.g., the right to erasure) in certain circumstances due to legal obligations or reasons of public interest. However, requests from individuals will be handled in accordance with the UK GDPR.

8. Sharing and Disclosure of Data

Special Category Personal Data and Criminal Offence Data may only be shared with third parties where it is necessary and lawful to do so. All third-party recipients of such data must agree to implement appropriate safeguards and ensure the data will be processed in compliance with the UK GDPR.

Third-party sharing may occur in the following circumstances:

- When required by law or regulatory bodies
- When necessary to fulfil public interest functions
- When necessary to perform a contract with the data subject or to protect vital interests

The Council will assess each request for data sharing on a case-by-case basis to ensure compliance with data protection laws.

9. Training and Awareness

The Council will provide appropriate training to all staff handling Special Category Personal Data and Criminal Offence Data to ensure they understand the importance of data protection and their responsibilities under this policy. This training will be reviewed and updated regularly.

All staff members involved in the processing of Special Category Personal Data and Criminal Offence Data must:

- Be familiar with this policy and understand their obligations under the UK GDPR.
- Ensure that data is processed securely and in compliance with this policy.
- Report any data protection concerns or breaches immediately to the Data Protection Officer.
- Complete mandatory data protection training to understand the importance of data privacy and security.

10. Data Breaches and Incident Management

In the event of a data breach involving Special Category Personal Data or Criminal

Offence Data, the Council will:

- Immediately notify the Data Protection Officer and initiate the data breach management procedures.
- Assess the severity and potential impact of the breach on individuals and take appropriate action, including informing affected individuals if the breach is likely to result in high risks to their rights and freedoms.
- Notify the Information Commissioner's Office (ICO) within 72 hours of the Council being notified where required and provide them with full details of the breach.
- Mitigate the risks of the breach by implementing corrective actions and strengthening security measures.

11. Contact Information

For questions or more information about this policy, please contact the Data Protection Officer.

12. Monitoring and Review

This policy will be formally reviewed every three years or when there are significant changes in the law or Three Rivers District Council procedures.

THREE RIVERS
DISTRICT COUNCIL