BEDFORD BOROUGH COUNCIL

Appropriate Policy Document (APD)

Bedford Borough Council is committed to protecting personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This Appropriate Policy Document (APD) explains how we process special category personal data and criminal offence data. It also sets out the procedures we follow to comply with data protection law, including how we retain and delete this information.

November 2026

Chief Executive

Scope

As part of our statutory duties, corporate functions and public tasks, we process special category personal data and criminal offence data in accordance with:

- Articles 9 and 10 of the UK General Data Protection Regulation (UK GDPR)
- Schedule 1 of the Data Protection Act 2018 (DPA 2018)

Some conditions in Schedule 1 of the Data Protection Act 2018 require us to have an Appropriate Policy Document in place.
This document explains our processing activities and meets the requirements of Schedule 1, Part 4 of the Data Protection Act 2018.

Special category personal data

Special category personal data is defined in Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Health data
- Data concerning a person's sex life or sexual orientation

Criminal offence data

Criminal offence data is described in Article 10 of the UK GDPR as any personal data relating to criminal convictions and offences or related security measures.

Section 11(2) of the Data Protection Act 2018 confirms that this also includes personal data relating to:

- the alleged commission of offences
- proceedings for an offence committed or alleged to have been committed
- sentencing.

Throughout this document, this information is referred to as criminal offence data.

How we use this information

The council processes special category personal data and criminal offence data when carrying out its statutory duties, corporate functions and public services, including, but not limited to:

- Adult Social Care
- Children's Services
- Public Health
- Education
- Employment and workforce management
- Legal, regulatory and enforcement activities.

Further information is available in the council's privacy statements.

Conditions for processing special category personal data

We process special category personal data under the following provisions of the UK GDPR:

- Article 9(2)(a) – explicit consent for one or more specified purposes
- Article 9(2)(b) – employment, social security and social protection
- Article 9(2)(c) – protection of the vital interests of the data subject
- Article 9(2)(f) – establishment, exercise or defence of legal claims
- Article 9(2)(g) – reasons of substantial public interest
- Article 9(2)(h) – health or social care (with a basis in law)
- Article 9(2)(i) – public health (with a basis in law)
- Article 9(2)(j) – archiving, research or statistics

Where we process special category personal data under certain UK GDPR provisions, we also rely on conditions in Schedule 1 of the Data Protection Act 2018.

Employment, social security and social protection

For processing under Article 9(2)(b), we rely on the condition in Schedule 1, Part 1, Paragraph 1 of the Data Protection Act 2018.

Reasons of substantial public interest

For processing under Article 9(2)(g), we rely on relevant conditions in Schedule 1, Part 2 of the Data Protection Act 2018.

Where appropriate, the council relies on:

- Schedule 1, Part 2, Paragraph 6 – Statutory and government purposes
- Schedule 1, Part 2, Paragraph 8 – Equality of opportunity or treatment
- Schedule 1, Part 2, Paragraph 10 – Preventing or detecting unlawful acts
- Schedule 1, Part 2, Paragraph 11 – Protecting the public against dishonesty, malpractice or improper conduct
- Schedule 1, Part 2, Paragraph 18 – Safeguarding children and individuals at risk.

Health or social care

For processing under Article 9(2)(h), we rely on the condition in Schedule 1, Part 1, Paragraph 2 of the Data Protection Act 2018.

Public health

For processing under Article 9(2)(i), we rely on the condition in Schedule 1, Part 1, Paragraph 3 of the Data Protection Act 2018.

Archiving, research and statistics

For processing under Article 9(2)(j), we rely on the condition in Schedule 1, Part 1, Paragraph 4 of the Data Protection Act 2018.

Conditions for processing criminal offence data

We process criminal offence data under Article 10 of the UK GDPR.

Where required, we rely on the relevant conditions contained in Schedule 1, Part 3 of the Data Protection Act 2018.

Where we process criminal offence data for law enforcement purposes and under the control of an official authority, the processing is covered by Part 3 of the Data Protection Act 2018. In these circumstances, we are not required to identify a Schedule 1 condition for processing.

Procedures for securing compliance

Article 5 of the UK GDPR sets out the data protection principles. These principles underpin how we collect, use, store and dispose of personal information.

Principle (a): Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner.

The council will:

- ensure personal data is processed only where a lawful basis applies
- process personal data fairly and ensure people are not misled about how their information is used
- provide clear privacy information so people understand how their information is processed.

Principle (b): Purpose limitation

Personal data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The council will:

- collect personal data only for specified, explicit and legitimate purposes
- explain those purposes through privacy notices
- not use personal data for incompatible purposes
- inform individuals before using personal data for a new compatible purpose.

Principle (c): Data minimisation

Personal data will be adequate, relevant and limited to what is necessary for the purposes for which it is processed.

The council will:

- collect only the personal data needed for a specific purpose
- ensure the information collected is adequate and relevant

Principle (d): Accuracy

Personal data will be accurate and, where necessary, kept up to date.

The council will:

- take reasonable steps to keep personal data accurate
- update information where necessary
- take particular care where the use of personal data could significantly affect individuals.

Principle (e): Storage limitation

Personal data will be kept in a form that permits identification of individuals for no longer than is necessary for the purposes for which it is processed.

The council will:

- keep personal data only for as long as it is needed
- retain information longer only where there is a legal requirement to do so

- securely delete or permanently anonymise information when it is no longer required.

Principle (f): Integrity and confidentiality (security)

Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The council will:

- maintain appropriate organisational and technical security measures
- protect personal data throughout its lifecycle
- regularly review security arrangements and controls.

Accountability principle

The council must be able to demonstrate compliance with data protection law.

The council will:

- maintain Records of Processing Activities in accordance with Article 30 UK GDPR
- carry out Data Protection Impact Assessments for high-risk processing and consult the Information Commission where required
- ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of the council's handling of personal data, has access to the highest level of management and has the resources needed to carry out the role
- provide mandatory data protection and information security training to employees and relevant contractors
- maintain policies, procedures and processes to ensure personal data is collected, used and handled in compliance with data protection law.

Retention and erasure of personal data

Where special category personal data or criminal offence data is processed, the council will ensure that:

- records of processing are maintained and, where possible, include the expected retention period for different categories of data
- retention and disposal arrangements follow the council's Records Retention and Disposal Schedule
- information is deleted or permanently anonymised when it is no longer required, unless there is a legal obligation to retain it
- privacy information explains how long personal data will be retained, or the criteria used to determine retention periods.

Security and safeguards

Bedford Borough Council implements technical and organisational security measures to protect personal data, including:

- Access controls to limit who can access sensitive data
- Encryption and pseudonymisation where applicable
- Secure storage and transfer methods

Data Subject Rights

Individuals whose data is processed by Bedford Borough Council have the following rights under the UK GDPR:

- Right to be informed about how their data is used
- Right of access to their data
- Right to rectification of inaccurate or incomplete data
- Right to erasure in certain circumstances
- Right to restriction of processing in some cases
- Right to data portability (where applicable)
- Right to object to processing in some cases
- Rights in relation to automated decision-making and profiling

Contact information

For any queries about this policy or data protection at Bedford Borough Council, contact:

The Data Protection Officer (DPO)
Bedford Borough Council
Borough Hall
Cauldwell Street
Bedford
MK42 9AP

Email: dpo@bedford.gov.uk

Review and updates

This Appropriate Policy Document will be reviewed regularly and updated as necessary to ensure ongoing compliance with data protection laws.

Last Updated: November 2026