CARLTON COLVILLE TOWN COUNCIL
DATA PROTECTION POLICY

To be reviewed: May 2027

Purpose

Carlton Colville Town Council ("the Council") is committed to protecting personal data and processing information fairly, lawfully, transparently and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) where applicable, and guidance issued by the Information Commissioner's Office (ICO).

This policy explains how the Council collects, stores, uses and protects personal data relating to councillors, employees, contractors, volunteers, residents, suppliers and other individuals who interact with the Council.

The Council recognises its responsibilities as a data controller and is committed to ensuring that all personal data is handled in line with current legislation and good governance practices.

The Clerk to the Council is responsible for overseeing data protection compliance, maintaining records of processing activities and acting as the primary point of contact for data protection matters.

Definitions

"Personal data" means any information relating to an identified or identifiable living individual.

"Special category data" includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

"Processing" means any operation performed on personal data including collection, storage, use, disclosure, sharing, amendment or destruction.

"Data subject" means the individual to whom personal data relates.

"Data controller" means the organisation that determines the purposes and means of processing personal data.

"Data processor" means any person or organisation processing data on behalf of the controller.

Data Protection Principles

The Council will comply with the principles set out in Article 5 of the UK GDPR. Personal data shall be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- retained only for as long as necessary;
- processed securely using appropriate technical and organisational measures; and
- processed in a manner that demonstrates accountability and compliance.

The Council maintains appropriate privacy notices and records of processing activities as required by law.

Lawful Basis for Processing

The Council processes personal data only where a lawful basis applies under Article 6 of the UK GDPR. These may include:

- compliance with a legal obligation;
- performance of a public task carried out in the public interest;
- performance of a contract;
- legitimate interests pursued by the Council or a third party;
- protection of vital interests; or
- consent where required.

Special category data will only be processed where an additional condition under Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018 applies.

Individual Rights

Individuals have the following rights under UK data protection legislation:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure in certain circumstances;
- the right to restrict processing;
- the right to data portability where applicable;

• the right to object to processing; and
• rights relating to automated decision-making and profiling.

Requests relating to personal data should be submitted to the Clerk. The Council will normally respond within one calendar month.

Individuals also have the right to complain to the Information Commissioner's Office:
Website: https://www.ico.org.uk

Data Sharing and Disclosure

The Council may share personal data with professional advisers, payroll providers, IT service providers, government bodies, auditors, insurers and other organisations where there is a lawful basis to do so.

All third-party processors acting on behalf of the Council must provide sufficient guarantees regarding security and confidentiality and must process data only on documented instructions from the Council.

Data Retention

The Council will retain personal data only for as long as necessary and in accordance with legal, regulatory and operational requirements. Retention periods will follow the Council's approved retention schedule and guidance issued by the National Association of Local Councils (NALC) and the ICO where appropriate.

At the end of the retention period, personal data will be securely deleted, destroyed or anonymised.

Information Security

The Council takes appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, loss or destruction.

Security measures include, where appropriate:

• password protection and multi-factor authentication;
• secure storage of paper and electronic records;
• encryption of portable devices and sensitive files;
• restricted access based on business need;
• secure disposal of confidential waste;
• staff awareness and training; and
• regular review of cyber security arrangements.

Any suspected security incident or data breach must be reported immediately to the Clerk.

Personal Data Breaches

The Council will investigate all personal data breaches promptly and maintain an internal breach log.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Council will report the breach to the Information Commissioner's Office within 72 hours of becoming aware of it.

Where a breach is likely to result in a high risk to affected individuals, those individuals will also be informed without undue delay.

International Transfers

The Council will not transfer personal data outside the United Kingdom unless appropriate safeguards are in place in accordance with UK GDPR requirements, including adequacy regulations, standard contractual clauses or other approved transfer mechanisms.

Training and Responsibilities

All councillors, employees, contractors and volunteers who process personal data on behalf of the Council are responsible for complying with this policy and associated procedures.

Individuals handling personal data must:

- access information only where authorised;
- keep information secure and confidential;
- avoid sharing personal data unnecessarily;
- report suspected breaches promptly; and
- complete relevant training where required.

Failure to comply with this policy may result in disciplinary action and, where appropriate, legal action.

Monitoring and Review

This policy will be reviewed annually or earlier where legislative or operational changes require amendments.

Approved by Carlton Colville Town Council.