DATA PROTECTION POLICY

YEOVIL TOWN COUNCIL

YEOVIL TOWN COUNCIL

DATA PROTECTION POLICY

1. Introduction

1.1 The Council processes a wide range of information in order to carry out its statutory duties and services.

1.2 This includes personal data relating to staff, councillors, residents, and service users.

1.3 The Council is committed to:

- Protecting personal data and confidentiality
- Being transparent about how data is used
- Complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018

1.4 This policy outlines the Council's approach to handling information securely, lawfully, and responsibly.

2. Definitions

2.1 Personal Data: Information relating to an identifiable individual

2.2 Special Category Data: Sensitive data such as health, ethnicity, political views or criminal records

2.3 Processing: Any activity involving personal data (collection, storage, use or deletion)

2.4 Business Purposes: Administrative, financial, statutory, payroll, service delivery and operational Council functions

3. Scope

3.1 This policy applies to all councillors, employees, contractors and volunteers.

3.2 All must comply with its provisions.

3.3 It also applies to all information held by the Council, including:

- Personal data
- Special category data
- Confidential and commercially sensitive information
- Information in electronic or paper format

4. Types of Information Processed

4.1 The Council processes:

- Public data – information required to be published
- Confidential data – draft policies, internal business
- Personal data, including:
  - Staff and councillor records
  - Resident enquiries, complaints, and service requests
  - Contracts and financial transactions

5. Data Protection Principles

5.1 The Council will ensure personal data will be:

- Lawful, fair and transparent
- Collected for specified purposes
- Adequate, relevant and limited
- Accurate and up to date
- Retained only as necessary
- Secure and protected

6. Lawful Basis for Processing

6.1 The Council will only process personal data where a lawful basis applies, including:

- Legal obligation
- Public task
- Contract
- Consent (where required)

6.2 The Council maintains a Record of Processing Activities (ROPA) which links all processing activities to their lawful basis.

6.3 Where consent is relied upon:

- It must be freely given, specific and recorded
- Individuals may withdraw consent at any time

7. Special Category Data

7.1 Special category data will be:

- Processed only where strictly necessary
- Subject to additional safeguards
- Supported by a lawful condition under GDPR

8. Operational Procedures for Data Processing

8.1 All processing must:

- Be necessary for Council functions
- Be proportionate and relevant
- Have an identified lawful basis
- Follow data minimisation principles (only necessary data collected)

8.2 Before starting new processing:

- The Data Protection Officer (DPO) must be consulted
- DPIAs must be completed where required
- Privacy notices must be updated

9. Individual Rights

9.1 Individuals have the right to:

- Be informed
- Access their data (Subject Access Request)
- Rectification
- Erasure
- Restrict processing
- Object
- Data portability

9.2 Requests will be handled within statutory timeframes and recorded.

9.3 Individuals have the right to complain to the Information Commissioner's Office (ICO). They can be contacted at:

- www.ico.org.uk, or
- in writing to:

  Information Commissioner's Office
  Wycliffe House Water Lane
  Wilmslow
  Cheshire
  SK9 5AF

10. Subject Access Requests (SARs) – Procedure

10.1 Requests must be sent immediately to the DPO.

10.2 Identity must be verified.

10.3 Relevant data identified and retrieved.

10.4 Response issued within statutory deadlines.

10.5 Records of requests must be retained.

11. Roles and Responsibilities

11.1 Council (Data Controller)

11.1.1 The Council is the Data Controller, responsible for ensuring compliance.

11.2 Data Protection Officer

11.2.1 The Chief Executive / Town Clerk acts as the Data Protection Officer (DPO).

11.2.2 They are responsible for:

- Providing guidance to staff and councillors
- Monitoring compliance and risks
- Maintaining records of processing
- Handling SARs and breaches
- Approving third-party agreements
- Liaising with the ICO

11.3 Councillors and Staff

11.3.1 All must:

- Follow this policy
- Handle data securely
- Ensure accuracy
- Report any breaches immediately

12. Data Security

12.1 General Security Measures

12.1.1 The Council will ensure appropriate technical and organisational security measures, including:

- Password-protected systems
- Secure storage (digital and physical)
- Restricted access on a “need to know” basis
- Encryption where appropriate

12.2 Detailed Handling Rules

- Paper records:
  - Stored securely and locked
  - Not left unattended
  - Shredded when no longer required

- Electronic data:
  - Protected by strong passwords
  - Not stored on unsecured devices
  - Encrypted where appropriate
- Portable devices:
  - Must be authorised and secured
  - Encrypted where possible

12.3 Data must be protected against:

- Unauthorised access
- Loss or destruction
- Misuse or disclosure

13. IT and Security Responsibilities

13.1 Systems must meet security standards

13.2 Data must be backed up regularly

13.3 Cloud services must be approved by the DPO

13.4 Third-party systems must be secure

14. Accuracy and Data Quality

14.1 Data must be accurate and kept up to date

14.2 Incorrect data must be corrected promptly

14.3 Disputes about accuracy must be recorded and reported

15. Information Handling

15.1 The Council will ensure:

- Data is used only for legitimate purposes
- Access is limited to authorised users
- Personal devices are secured if used for council business

15.2 All records must be:

- Stored securely
- Safely disposed of when no longer required

16. Data Sharing

16.1 Personal data will only be shared:

- Where necessary

- Where a lawful basis exists
- Minimum necessary data will be shared
- Third parties must have appropriate safeguards

16.2 Third-Party Processing:

- Must be governed by a formal agreement
- Must be approved by the DPO
- Must meet required security standards

17. Direct Marketing and Communications

- Individuals may opt out of marketing
- Marketing must comply with lawful basis requirements
- DPO must be consulted before campaigns

18. Data Retention

18.1 Personal data will:

- Be retained only as long as necessary
- Follow the Council's Retention Policy
- Be securely destroyed when no longer required

19. Data Breaches

- A data breach includes loss, theft or unauthorised disclosure of data

19.1 All breaches must be reported immediately to the DPO.

19.2 The Council will:

- Record all breaches
- Assess risk
- Report serious breaches to the ICO within 72 hours where required

19.3 Affected individuals will be informed where necessary.

20. Data Protection Impact Assessment (DPIAs)

20.1 The Council will carry out DPIAs where processing:

- Is high risk
- Involves new systems or technologies

20.2 DPIAs will identify and mitigate risks to individuals' rights.

21. Privacy Notices

21.1 The Council will maintain clear Privacy Notices explaining:

- What data is collected
- Why it is collected
- How it is used
- How long it is retained

21.2 Privacy Notices will be:

- Published on the Council website
- Reviewed regularly

22. Publication Scheme and Transparency

22.1 The Council will:

- Publish information in line with its Publication Scheme
- Provide non-confidential information openly to the public

23. ICO Registration

23.1 The Council will:

- Register with the Information Commissioner's Office
- Pay the required data protection fee

23.2 The Council maintains a Record of Processing Activities (ROPA) including:

- Purposes of processing
- Categories of data subjects and personal data
- Recipients of data
- Retention periods
- Security measures

24. International Data Transfers

24.1 The Council does not routinely transfer personal data outside the UK.

24.2 Where such transfers occur, appropriate safeguards will be implemented in accordance with UK GDPR.

25. Processing on Behalf of Others

25.1 Where the Council processes personal data on behalf of another organisation, it will comply with processor obligations under UK GDPR and ensure appropriate contractual controls are in place.

26. Children's Data

26.1 Where the Council processes children's data, additional care will be taken to ensure it is protected appropriately and processed lawfully.

27. Training and Awareness

27.1 The Council will ensure:

- Appropriate data protection training for staff and councillors
- Ongoing awareness of legal responsibilities

28. Monitoring and Review

28.1 This policy will be:

- Reviewed annually
- Updated in line with legislation and guidance

28.2 Compliance will be monitored through:

- Internal controls
- Audit processes (including AGAR requirements)

29. Review

29.1 This policy will be reviewed annually by the Council.

Yeovil Town Council
September 2026
To be reviewed: September 2027