

BURY ST EDMUNDS

TOWN COUNCIL

DATA PROTECTION POLICY

Data Protection Policy

1. Purpose

Bury St Edmunds Town Council is committed to protecting personal data and respecting the privacy rights of residents, councillors, employees, volunteers, contractors, suppliers, grant applicants, service users and other individuals whose information it handles. This policy sets out how the Council will comply with the UK General Data Protection Regulation, the Data Protection Act 2018 and related information rights legislation.

2. Scope

This policy applies to all personal data processed by or on behalf of the Council, whether held electronically, on paper, in images, audio, video, emails, forms, databases, minutes, correspondence or any other format. It applies to councillors, employees, volunteers, contractors, consultants, processors and any person acting under the authority of the Council.

3. Definitions

- **Personal data** means information relating to an identified or identifiable living individual.
- **Special category data** includes information about health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, sex life or sexual orientation.
- **Processing** means any operation carried out on personal data, including collecting, recording, storing, using, sharing, deleting or destroying it.
- **Data subject** means the individual whose personal data is being processed.
- **Controller** means the organisation that decides why and how personal data is processed.
- **Processor** means an organisation or person processing personal data on behalf of the controller.

4. Data Protection Principles

The Council will ensure that personal data is processed in accordance with the data protection principles. Personal data must 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; kept for no longer than necessary; and processed securely. The Council must also be able to demonstrate compliance through appropriate records, policies, procedures and governance arrangements.

5. Roles and Responsibilities

- **Full Council** has overall responsibility for ensuring the Council complies with data protection legislation.
- **The Town Clerk** is responsible for day-to-day implementation of this policy, maintaining appropriate procedures, ensuring staff and councillors receive guidance, and escalating significant data protection risks.
- **Employees, councillors and volunteers** must handle personal data lawfully, securely and only for authorised Council purposes.

- **Processors and contractors** must process personal data only under written instructions from the Council and must provide appropriate security and confidentiality safeguards.
- **The Data Protection Officer or appointed data protection lead, where applicable,** will advise on compliance, monitor implementation and act as a contact point for data protection matters.

6. Lawful Basis for Processing

The Council will identify and document an appropriate lawful basis before processing personal data. Depending on the purpose, processing may be based on public task, legal obligation, contract, consent, vital interests or legitimate interests where applicable. As a public authority, the Council will normally rely on public task or legal obligation for functions carried out in the public interest or under statutory duties. Consent will only be used where it is freely given, specific, informed and capable of being withdrawn.

7. Special Category and Criminal Offence Data

The Council will only process special category data or criminal offence data where there is a lawful basis and an additional condition under data protection legislation. Such data will be subject to higher levels of protection, restricted access and, where required, an appropriate policy document setting out safeguards and retention arrangements.

8. Privacy Information

The Council will provide clear privacy information explaining what personal data is collected, why it is used, the lawful basis, who it may be shared with, how long it is retained, individual rights and how to contact the Council. Privacy notices will be made available at the point personal data is collected wherever practicable and will be reviewed regularly.

9. Individual Rights

Individuals have rights in relation to their personal data, subject to legal conditions and exemptions. These include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights relating to automated decision-making and profiling. Requests must be passed promptly to the Town Clerk or designated data protection contact and handled within statutory timescales.

10. Subject Access Requests

A subject access request is a request from an individual for access to their personal data. Requests may be made verbally or in writing and do not need to use any particular wording. Any person receiving a request must forward it immediately to the Town Clerk or designated data protection contact. The Council will verify identity where necessary, search relevant records, consider any exemptions and respond within the required legal timeframe.

11. Data Accuracy and Minimisation

The Council will collect only the personal data needed for defined purposes and will take reasonable steps to ensure that personal data is accurate, complete and kept up to date. Personal data must not be collected or retained simply because it may be useful in the future.

12. Records Management and Retention

The Council will maintain appropriate records of processing activities and will retain personal data only for as long as necessary for the purpose for which it was collected, including any statutory, audit, financial, employment, safeguarding or legal requirements. Personal data must be securely deleted, destroyed or anonymised when no longer required. Retention arrangements should be documented in a retention schedule and reviewed regularly.

13. Information Security

- Personal data must be stored securely and accessed only by authorised persons who need it for Council business.
- Electronic records must be protected by appropriate passwords, permissions, backups, antivirus protection and secure systems.
- Paper records must be kept securely and disposed of using confidential waste arrangements where appropriate.
- Personal data must not be sent to personal email accounts or stored on unmanaged personal devices unless specifically authorised and protected.
- Emails containing personal data must be checked carefully before sending and must use secure methods where the sensitivity of the data requires it.
- Lost, stolen or misdirected information must be reported immediately as a potential personal data breach.

14. Data Sharing

The Council will only share personal data where there is a lawful basis, a clear purpose and appropriate safeguards. Data may be shared with public authorities, professional advisers, insurers, auditors, payroll providers, IT providers, grant funders, contractors or other organisations where necessary for Council functions or legal obligations. Where regular or significant sharing takes place, the Council will use appropriate data sharing agreements or contractual clauses.

15. Processors and Contracts

Where the Council appoints a processor to process personal data on its behalf, the Council will carry out proportionate due diligence and ensure that a written contract is in place. Contracts must require the processor to act only on the Council's documented instructions, protect personal data, assist with individual rights and breaches, use approved sub-processors only where authorised, and return or delete personal data at the end of the service.

16. International Transfers

The Council will not transfer personal data outside the United Kingdom unless appropriate safeguards are in place and the transfer complies with data protection legislation. Where cloud, software or external services involve international transfers, the Council will assess the arrangements before use.

17. Data Protection by Design and Default

The Council will consider data protection at the start of any new project, service, system, contract, event, consultation or processing activity. Privacy risks will be assessed and appropriate measures built in from the outset. This includes limiting data collection, restricting access, using secure systems, providing privacy information and setting retention periods.

18. Data Protection Impact Assessments

A Data Protection Impact Assessment will be completed where processing is likely to result in a high risk to individuals' rights and freedoms. This may include new technologies, large-scale processing, systematic monitoring, processing special category data, CCTV or other activities that may significantly affect individuals. High risks that cannot be mitigated must be escalated and, where required, referred to the Information Commissioner's Office before processing begins.

19. Personal Data Breaches

A personal data breach is a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include lost papers, emails sent to the wrong recipient, unauthorised access, cyber incidents, stolen devices or accidental deletion. All suspected breaches must be reported immediately to the Town Clerk or designated data protection contact. The Council will record breaches, assess risk, take containment action and, where required, report to the Information Commissioner's Office within 72 hours of becoming aware of a reportable breach. Affected individuals will be informed where the breach is likely to result in a high risk to their rights and freedoms.

20. CCTV, Photographs and Recordings

Where the Council uses CCTV, photographs, video or audio recordings, it will ensure that use is necessary, proportionate, transparent and supported by appropriate notices, procedures and retention arrangements. Images and recordings that identify individuals are personal data and must be handled in accordance with this policy.

21. Employment and Councillor Information

The Council will process employee, volunteer and councillor information only for legitimate employment, governance, statutory, safeguarding, health and safety, payroll, pension, training, disciplinary, complaints, audit and administration purposes. Access will be restricted to those with a business need, and individuals will be provided with appropriate privacy information.

22. Training and Awareness

The Council will ensure that employees, councillors and relevant volunteers or contractors receive appropriate data protection awareness, guidance and training. Training will be proportionate to the role and the type of personal data handled. Individuals must understand their responsibilities for confidentiality, security, recognising rights requests and reporting breaches.

23. Monitoring and Compliance

Compliance with this policy will be monitored through governance checks, review of processing records, breach records, contracts, privacy notices, training records and retention arrangements. Any significant risks or repeated non-compliance will be reported to the appropriate Council committee or Full Council.

24. Complaints and Contact

Individuals who have questions or concerns about how the Council handles their personal data should contact the Town Clerk in the first instance. Individuals also have the right to complain to the Information Commissioner's Office if they are dissatisfied with the Council's response or believe their data protection rights have been infringed.

25. Review

This policy will be reviewed annually, or sooner if there are changes to legislation, statutory guidance, Council services, systems, suppliers, risks or processing activities. Amendments will be approved through the Council's governance arrangements.

Appendix A: Practical Staff and Councillor Checklist

- Only collect personal data that is needed for a clear Council purpose.
- Use personal data only for the purpose for which it was collected, unless a compatible lawful purpose applies.
- Keep personal data accurate and update it where necessary.
- Store personal data securely and restrict access to those who need it.
- Do not disclose personal data unless authorised and lawful.
- Use secure methods when sending sensitive information.
- Report suspected data breaches immediately.
- Forward rights requests promptly to the Town Clerk or designated contact.
- Delete, destroy or archive personal data in line with the Council's retention schedule.
- Ask for advice before starting any new activity involving personal data.