SUDBURY TOWN COUNCIL

DATA PROTECTION POLICY

1. PURPOSE

Sudbury Town Council (STC) is committed to protecting the rights and freedoms of individuals in relation to the processing of personal data and complying with the requirements of:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations (PECR)
- Relevant guidance issued by the Information Commissioner's Office (ICO)
- Any other applicable legislation and regulatory requirements relating to information governance and data protection

This policy explains how STC collects, uses, stores, shares and disposes of personal data and outlines the responsibilities of councillors, employees, contractors, volunteers and third parties who process personal data on behalf of STC.

STC recognises that good information governance is essential to maintaining public confidence and delivering services lawfully, securely and transparently.

2. SCOPE

This policy applies to:

- Employees
- Councillors
- Contractors
- Consultants
- Volunteers
- Agency Workers
- Anyone processing personal data on behalf of STC

This policy applies to all personal data processed by STC regardless of format including:

- Electronic records
- Paper files
- Audio recordings
- CCTV images

- Emails and correspondence
- Cloud-based systems
- Mobile devices

This policy should be read alongside our other policies relating to internet use, email, CCTV, body-worn cameras, and trail cameras.

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

3. DEFINITIONS

Personal Data

Any information relating to an identified or identifiable living individual. Examples include:

- Names
- Addresses
- Email addresses
- Telephone numbers
- Identification numbers
- Payroll information
- HR records
- Online identifiers
- Photographs

Special Category Data

Personal data requiring additional protection under UK GDPR, including:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data
- Biometric data used for identification
- Health information
- Sexual orientation or sex life

Criminal Offence Data

Information relating to criminal convictions, offences, allegations or related security measures.

Processing

Any operation carried out on personal data including collection, storage, use, disclosure, sharing, deleting or destruction.

Data Subject

The individual to whom personal data relates.

4. DATA PROTECTION PRINCIPLES

STC will comply with the UK GDPR principles by ensuring personal data is:

- 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 only for as long as necessary
- Processed securely using appropriate technical and organisational measures

STC will also demonstrate accountability by maintaining appropriate records, policies, procedures and governance.

5. LAWFUL BASIS FOR PROCESSING

Before processing personal data STC will identify and document an appropriate lawful basis under Article 6 UK GDPR.

STC primarily processes personal data under the following lawful bases:

- Public Task
- Legal Obligation
- Contract
- Vital Interests
- Legitimate Interests (where appropriate and balanced against individuals' rights).

Consent will only be relied upon where it can be freely given, specific, informed and capable of withdrawal.

Where special category data is processed, the Council will identify an additional condition for processing under Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018.

6. TRANSPARENCY AND PRIVACY NOTICES

STC will provide clear and accessible privacy notices explaining:

- What personal data is collected
- Why it is collected
- The lawful basis for processing
- How the information will be used
- Who it may be shared with
- How long it will be retained
- Individuals' rights
- How to contact the Council and the ICO.

Privacy notices will be reviewed regularly and updated where necessary.

7. INDIVIDUAL RIGHTS

Individuals have the following rights under UK GDPR:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making and profiling.

The Council will respond to valid requests without undue delay and normally within one calendar month.

The Council may request proof of identity before responding to requests.

Individuals have the right to complain to the Information Commissioner's Office if they are dissatisfied with how their personal data has been handled.

8. SUBJECT ACCESS REQUESTS

Any individual may request access to personal data held about them.

All Subject Access Request (SARs) must be forwarded immediately to the Person Responsible for Data Protection.

STC will:

- Acknowledge requests promptly
- Verify the identity of the requester where appropriate
- Respond within one calendar month unless an extension is permitted under law
- Provide information free of charge unless the request is manifestly unfounded or excessive.

Where exemptions apply, STC may withhold information in accordance with applicable legislation.

A record of all SARs will be maintained.

9. ROLES AND RESPONSIBILITIES

STC

STC is the Data Controller for personal data processed in connection with its functions and services.

Person Responsible for Data Protection

The Council has appointed a Person Responsible for Data Protection. They are responsible for:

- Monitoring compliance with data protection legislation
- Advising the Council on data protection obligations
- Supporting Data Protection Impact Assessments (DPIAs)
- Providing guidance and training
- Monitoring breaches and incidents
- Acting as the contact point for the ICO and data subjects

The Person Responsible for Data Protection shall operate independently and report directly to senior management or Full Council where necessary.

Managers

Managers are responsible for ensuring that:

- All staff understand and comply with this policy
- Appropriate security measures are implemented
- Personal data is processed lawfully
- Data protection risks are identified and managed

All Councillors, Employees and Workers

All individuals covered by this policy must:

- Process personal data only where authorised
- Keep personal data secure and confidential
- Report actual or suspected data breaches immediately
- Complete mandatory training
- Follow STC procedures and guidance

10. INFORMATION SECURITY

STC will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Security measures include:

- Strong password requirements
- Multi-factor authentication (MFA) where appropriate
- Encryption of devices and sensitive information
- Secure backups
- Access controls based on business need
- Anti-virus and endpoint protection
- Firewalls and network security
- Secure disposal of records and equipment
- Secure remote working arrangements
- Monitoring and auditing of systems

Personal data stored on laptops, tablets or mobile devices must be encrypted and protected in accordance with STC information technology security requirements.

Paper records containing personal data must be stored securely and shredded or confidentially disposed of when no longer required.

The use of removable media such as USB devices must be authorised and appropriately secured.

11. REMOTE AND HYBRID WORKING

Where staff work remotely or in hybrid arrangements, they must:

- Use council-approved devices and systems
- Ensure screens are locked when unattended
- Prevent unauthorised viewing or disclosure of information
- Store paper files securely
- Report lost or stolen devices immediately

Public Wi-Fi should not be used for processing sensitive personal data unless secure VPN access is in place and with prior agreement by the Person Responsible for Data Protection or the Town Clerk.

12. DATA SHARING AND THIRD-PARTY PROCESSORS

STC may share personal data where lawful and necessary with:

- Government bodies
- Regulatory authorities

- Other local authorities
- Professional advisers
- Contractors and service providers

Where third parties process personal data on behalf of STC, appropriate written agreements compliant with Article 28 UK GDPR must be in place.

STC will undertake appropriate due diligence on suppliers and processors, including consideration of:

- Information security standards
- Cyber security arrangements
- Data handling procedures
- International data transfers

Personal data will not be transferred outside the UK unless appropriate safeguards are in place.

13. DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

Data protection and privacy considerations must be embedded into projects, systems and processes from the outset.
STC will undertake Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to individuals. Examples include:

- New IT systems
- CCTV projects
- Large-scale data sharing
- Use of special category data
- New technologies
- Artificial intelligence or automated processing

The Person Responsible for Data Protection or the Town Clerk must be consulted before any significant new processing activity commences.

14. ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

Where artificial intelligence (AI), automated tools or data analytics are used, STC will ensure:

- Processing remains lawful, fair and transparent
- Human oversight is maintained
- Risks are assessed through DPIAs where required
- Bias and discrimination risks are considered

- Appropriate safeguards are implemented

STC will not undertake solely automated decisions with legal or similarly significant effects unless authorised by law and compliant with UK GDPR.

15. RECORDS MANAGEMENT AND RETENTION

STC will maintain records of processing activities and retain personal data only for as long as necessary. Retention periods will be determined in accordance with:

- Legal and regulatory requirements
- Operational need
- ICO guidance
- NALC guidance
- The Council's retention schedule

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

Retention schedules will be reviewed periodically.

16. DATA ACCURACY

STC will take reasonable steps to ensure personal data is accurate and up to date. Individuals are encouraged to notify the Council of changes to their personal information. Where inaccurate information is identified, it will be corrected or updated promptly.

17. PERSONAL DATA BREACHES

All actual or suspected personal data breaches must be reported immediately to the Person Responsible for Data Protection. Examples include:

- Loss or theft of devices or paperwork
- Sending information to the wrong recipient
- Unauthorised access to systems
- Cyber attacks
- Disclosure of confidential information

STC will:

- Investigate breaches promptly
- Maintain a breach register
- Assess risks to individuals

- Implement remedial measures
- Notify the Information Commissioner's Office (ICO) within 72 hours where legally required
- Notify affected individuals where there is a high risk to their rights and freedoms

Failure to report a breach may result in disciplinary action.

18. MARKETING AND COMMUNICATIONS

STC will comply with PECR and UK GDPR when undertaking electronic communications or marketing activities. STC will ensure that:

- Communications are lawful and proportionate
- Individuals can opt out where applicable
- Mailing lists are maintained securely
- Consultation and community engagement activities are transparent

Direct marketing communications will only be undertaken where lawful.

19. TRAINING

All councillors, employees and relevant contractors must complete mandatory data protection and information security training. Training will:

- Form part of the induction process
- Be refreshed annually
- Include cyber security awareness
- Cover phishing
- Be role specific

Completion of training is mandatory.

20. MONITORING, AUDIT AND COMPLIANCE

STC will monitor compliance with this policy through:

- Internal audits
- Risk assessments
- Compliance reviews
- Policy reviews
- Incident reporting
- DPIA monitoring

The Person Responsible for Data Protection will provide advice and recommendations to improve compliance and reduce risk.

21. CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with this policy may result in:

- Disciplinary action
- Withdrawal of system access
- Referral to regulatory authorities
- Legal proceedings where appropriate

Any deliberate or reckless misuse of personal data may constitute gross misconduct.

22. CONTACT DETAILS

Person Responsible for Data Protection
Sudbury Town Council
Town Hall
Old Market Place
Sudbury
Suffolk
CO10 1TL
Telephone: 01787 372331
Email: DPO@sudbury-tc.gov.uk

Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF
Telephone: 0303 123 1113
https://ico.org.uk/make-a-complaint/

SUDBURY
TOWN COUNCIL

DATA RETENTION POLICY

STC maintains a separate detailed Data Retention Schedule setting out:

- Categories of records held
- Minimum retention periods
- Disposal arrangements
- Legal and operational justification

The retention schedule will be reviewed regularly to ensure continued compliance with legislation and operational requirements.

DATA RETENTION SCHEDULE

Documentation	Minimum Retention Period	Justification (with references)
Minute Books	Indefinite	Archive
Receipt and Payment Accounts	Indefinite	Archive
Receipt Books (of all kinds)	6 years minimum (7 years adopted for admin consistency)	VAT requires this as a minimum
Bank Statements, including deposit / saving accounts	6 years minimum (7 years adopted for admin consistency)	Audit
Bank Paying-In Books	6 years minimum (7 years adopted for admin consistency)	Audit
Quotations and Tenders	7 years	Limitation Act 1980
Paid Invoices	6 years minimum (7 years adopted for admin consistency)	VAT requires this as a minimum
Paid Cheques	6 years minimum (7 years adopted for admin consistency)	Limitation Act 1980
VAT Records	6 years minimum (7 years adopted for admin consistency)	VAT requires this as a minimum
Petty Cash and Postage	6 years minimum (7 years adopted for admin consistency)	Tax, VAT and Limitation Act 1980
Timesheets	6 years minimum (7 years adopted for admin consistency)	Audit HMRC, NMW and Limitation Act 1980
Payroll Records	15 years	6 years minimum under HMRC/NMW requirements, but retained for 15 years for pension, employment and NI dispute purposes
Insurance Policies	40 years from date on which insurance was commenced or was renewed	Management
Certificates for Insurance (against liability for employees)	40 years from date on which insurance was commenced or renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (SI 2753)

Title Deeds, Leases, Agreements, Contracts	Indefinite	Audit Management
Members Allowances Register	6 years	Tax, Limitation Act 1980
Staff Related		
Personnel Files	6 years after end of employment	UK GDPR data minimisation principles and may be extended where litigation, safeguarding, pension or insurance issues apply
Records Relating to Disciplinary Proceedings	6 years after end of employment	UK GDPR data minimisation principles and may be extended where litigation, safeguarding, pension or insurance issues apply
Records of Recruitment for Unsuccessful Candidates	6 months after completion of the recruitment process	To defend against discrimination claims. This is because the time limit for discrimination claims is 3 months but takes into account a potential extension under the rules of early conciliation, it could be around 5 months before the employer hears of the claim against it
General Enquiries		
Any query taken in the office that may require personal details to respond	2 years unless correspondence forms part of a complaint, legal matter or contract	Management, because we might get a question up to 2 years after they contact us
Market		
Stall Holder Details	2 years	Management, because we might get a question up to 2 years after they leave the market
Events		
Stall Holder / Participant Details	2 years	Management, because we might get a question up to 2 years after they leave the market
Town Hall		
Applications to Hire	7 years	VAT
Lettings Diary	Indefinite	Archive

Invoices to Hirers	7 years	VAT
Allotments		
Waiting List	Remain while application remains active, review annually and remove inactive applicants after 2 years without response	Management UK GDPR
Allocation List	Indefinite	Current Information
Ex-plot Holders' Details	2 years after giving up the plot	Audit Management because we might get a question up to 2 years after they leave the plot
Cemetery		
Register of Fees Collected	7 years	Audit
Register of Burials	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)
Register / plan of grave plots	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)
Register of Memorials	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)
Notice of Interment	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)
Disposal Certificates	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)
Copy Certificates of Grant of Exclusive Right of Burial	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)
Applications for the right to erect memorials	Indefinite	Management, where linked to grave ownership records
Register of Purchased Graves	Indefinite	Archives Local Authorities Cemeteries Order 1977 (SI 204)

Retention periods shown are minimum periods. Records may be retained longer where required for legal proceedings, insurance claims, audit, safeguarding, pension administration, public interest archiving, or statutory inquiry purposes. Records containing personal data shall be reviewed in accordance with UK GDPR data minimisation principles.

Policy Name	Data Protection Policy inc. Data Retention Policy
Current Status	Adopted
Approved	September 2026
Next Review Date	July 2031
Policy Owner	Clare Morgan