

SUDBURY TOWN COUNCIL
MINUTES OF THE MEETING OF THE POLICY AND RESOURCES COMMITTEE HELD IN
SUDBURY TOWN HALL ON THURSDAY 18TH JULY 2024 AT 6.30PM

Committee members present: Mrs M Barrett – Chair
Mr S Hall
Ms E Murphy
Mrs J Osborne
Mr T Regester
Mr A Stohr
Mr A Welsh

Officers in attendance: Mr C Griffin – Town Clerk

1. SUBSTITUTES AND APOLOGIES

Apologies for absence were received from Councillor Mr P Beer. Ms E Murphy was the substitute for Mr Beer.

2. DECLARATIONS OF INTERESTS

Councillor Mr T Regester declared that he was a Babergh District Councillor.

3. DECLARATION OF GIFTS AND HOSPITALITY

No declarations of gifts or hospitality were made.

4. REQUESTS FOR DISPENSATION

No requests for dispensation had been received.

5. TO ELECT A VICE CHAIRMAN FOR THE COMMITTEE

It was proposed that Councillor Mr A Welsh be elected as the vice chairman of the committee for the year 2024/2025. There being no other nominations the motion was then put to a vote.

It was RESOLVED that Councillor Mr A Welsh be elected vice chairman of Policy and Resources Committee for the ensuing year.

6. MINUTES

RESOLVED

That the minutes of the Policy and Resources Committee meeting held on the 21st November 2023 be confirmed and signed as an accurate record.

7. ACTIONS FROM THE PREVIOUS MEETING

The Town Clerk advised that the main outstanding actions from the previous meeting were re-drafting of the terms of reference (TORs) for the committees. There would be no advantage in rushing these,

as the current TORs were adequate until better ones had been agreed. There were a number of areas that were not well covered in the current TORs, such as the business activities, and these needed careful thought as to how they should be covered in future.

RESOLVED

That the Town Clerk's report be noted.

8. STANDING ORDER 5(J)v

Members discussed the delegation arrangements to committees, sub-committees, staff and other local authorities. The delegations to committees were covered in their current TORs and these would be revised as discussed under item 7 above.

RESOLVED

That the delegation arrangements had been reviewed as required in Standing Order 5(J)v.

9. STANDING ORDER 5(J)vi

Members agreed that the delegations to committees were covered in their current TORs and these would be revised as discussed under item 7 above.

RESOLVED

That the delegation to committees had been reviewed as required in Standing Order 5(J)vi.

10. STANDING ORDER 5(J)viii

Members reviewed the need for new committees.

RESOLVED

That no new committees were required but that this could be reviewed once new TORs had been adopted.

11. STANDING ORDER 5(J)xi

Members considered representation on external bodies. The Town Clerk reminded members that this was an optional task, and that, if it were undertaken, members would represent the council to the other body and could not be advocates for the other body. They could not be members of the other body or have any close affiliation with it. A safer option would be for an officer of the council, such as the Business Manager, to represent the council at external bodies.

RESOLVED

That no member representation was currently required on external bodies and officers would routinely represent the council if required.

12. STANDING ORDER 5(J)xv

The members reviewed the council's subscriptions to other bodies in accordance with Standing Order 5(J)xv. These included the Suffolk Association of Local Councils (SALC), the Society of Local Council Clerks (SLCC), the Association of Accounting Technicians (AAT), the Information Commissioner's Office (ICO), the Institute of Cemetery and Crematorium Management (ICCM) and the National Association of British Market Authorities (NABMA).

RESOLVED

That the council's subscriptions to other bodies had been reviewed as required in Standing Order 5(J)xv.

13. STANDING ORDER 5(J)xvi

Members noted that there is currently a complaint being investigated and that they would review the Council's complaints procedure in the light of any lessons learnt.

RESOLVED

That Council's complaints procedure would be reviewed after the current complaint had been dealt with.

14. STANDING ORDER 5(J)xvii

The Council's policies, procedures and practices in respect of its obligations under freedom of information and data protection legislation were being considered as a separate item 16 on the agenda.

RESOLVED

The consider the revised data protection policy under item 16.

15. STANDING ORDER 5(J)xviii

Members reviewed the Council's policy for dealing with the press/media in accordance with Standing Order 5(J)xviii.

RESOLVED

That the Council's policy for dealing with the press and media was effective and there was no need to make changes.

16. TO REVIEW THE REVISED DATA PROTECTION POLICY

The revised draft of the Data Protection Policy shown below was discussed.

RESOLVED

To adopt the revised Data Protection Policy shown at **pages 495 to 505.**

17. TO REVIEW THE REVISED DOCUMENT RETENTION POLICY

Members agreed to move the document retention policy up in the agenda as it formed part of data protection. Members reviewed the table shown below and requested that best practice for CCTV images be brought back for inclusion as soon as possible.

RESOLVED

To adopt the revised Document Retention Policy shown at pages 506 to 508.

18. TO REVIEW THE REVISED SICKNESS ABSENCE POLICY

Members reviewed the revised sickness absence policy and made some changes to the draft to clarify the forms of contact during sickness absence.

RESOLVED

To adopt the revised Sickness Absence Policy shown at pages 509 to 519.

19. TO REVIEW THE POLICY FOR THE MAYOR’S EXPENSES

Members discussed how the Mayor’s expenses could best be divided between fixed tasks such as mayor making and discretionary events that the mayor chose to attend.

RESOLVED

That the Town Clerk draft some broad guidance for the allocation and use of the mayor’s allowance to clarify what was acceptable and to safeguard future mayors. This would be discussed at a future meeting.

20. TO AUTHORISE THE TOWN CLERK TO MAKE FACTUAL CHANGES TO EXISTING POLICIES, TO UPDATE THEM, WHEN NECESSARY, WITHOUT CHANGING THE SUBSTANCE OF THE POLICIES.

The Town Clerk explained that there were factual inaccuracies in some policies and that there was no way to correct these without bringing the matter back to the committee. As there could be long gaps between meetings, he recommended that he be given delegated authority to make factual changes to existing policies when necessary. This would not give him any authority to change the substance of the policy, only to correct problems. Examples included, changes of names, email addresses, dates, reference to external documents, or explanatory notes when a process was unclear. He proposed that every time he made such a change, he would send all members a revised copy with all the changes highlighted.

RESOLVED

To delegate authority to the Town Clerk to make factual changes to existing policies, to update them, when necessary, without changing the substance of the policies.

The meeting concluded at 8:21pm

.....
Chairman



SUDBURY TOWN COUNCIL

DATA PROTECTION POLICY

DRAFT

Introduction

We hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes.

This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

<p>Business purposes</p>	<p>The purposes for which personal data may be used by us:</p> <p>Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes.</p> <p><i>Council purposes include the following:</i></p> <ul style="list-style-type: none"> - <i>Compliance with our legal, regulatory and corporate governance obligations and good practice</i> - <i>Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests</i> - <i>Ensuring Council policies are adhered to (such as policies covering email and internet use)</i> - <i>Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking</i> - <i>Investigating complaints</i> - <i>Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments</i> - <i>Monitoring staff conduct, disciplinary matters</i> - <i>Promoting Council services</i> - <i>Improving services</i>
---------------------------------	--

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents, market traders, hirers, correspondents <i>Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records</i>
Sensitive personal data	<i>Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.</i>

Scope

This policy applies to all councillors and staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our Data Protection Officer, Mrs Debbie Deeks Administration Manager/s151 Officer, has overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the Council updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis

- Assisting with data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, council members and other stakeholders
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by Sudbury Town Council
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Officers

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice relating to on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers, employees, residents and service users
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that service users and correspondents have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Mrs Debbie Deeks, Administration Manager/s151 Officer.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the council's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data

was obtained, but should be determined in a manner consistent with our data retention guidelines.

Subject Access Requests

Please note that under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. Who may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

GDPR and Data Protection Act Provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	Staff at Sudbury Town Council
How is it collected?	Email, telephone, by hand
Why is it being collected?	For benefit claims, Universal Credit info, cemetery enquiries, event attendees
How will it be used?	For the sole purpose it is intended
Who will it be shared with?	Only info relating to Babergh District Council (BDC) matters will be shared with them
Identity and contact details of any data controllers	Debbie Deeks Debbie.deeks@sudbury-tc.gov.uk 01787 275773 www.sudbury-tc.gov.uk
Retention period	Anything relating to BDC will be deleted immediately after it's sent. All other information within 6 months.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in

breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

DRAFT

Annex B to Sudbury Town Council Data Protection Policy

SUDBURY TOWN COUNCIL

Data Retention Policy – Adopted 18 July 2024

Subject to any statutory or regulatory provision or advice from National or County associations (including that resulting from case law), the Town Council's policy for retaining data is as follows (in accordance with NALC guidelines at the time of coming into force):

DOCUMENT	MINIMUM RETENTION PERIOD	REASON (with reference)
Minute books	Indefinite	Archive
Receipt and payment account(s)	Indefinite	Archive
Receipt books of all kinds	7 years	VAT requires this as a minimum.
Bank statements, including deposit/saving accounts	7 years	Audit
Bank paying-in books	7 years	Audit
Cheque Book stubs	7 years	Audit
Quotations and tenders	7 years	Limitation Act 1980 (as amended)
Paid invoices	7 years	VAT
Paid cheques	7 years	Limitation Act 1980 (as amended)
VAT records	7 years	VAT
Petty cash, postage, and telephone books	7 years	Tax, VAT, limitation Act 1980 (as amended)
Timesheets	Last completed audit year	Audit
Payroll records	15 years	For Pension & National Insurance queries.

Insurance policies	40 years from date on which insurance commenced or was renewed	Management
Certificates for Insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (SI. 2753). Management.
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management
Members allowances register	6 years	Tax, Limitation Act 1980 (as amended).
Staff		
Personal files	6 years after end of employment	
Records relating to disciplinary proceedings	6 years after end of employment	
Records of recruitment for unsuccessful candidates	6 months after completion of the recruitment exercise.	To defend against discrimination claims. This is because the time limit for discrimination claims is three months but taking into account a potential extension under the rules on early conciliation, it could be around five 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	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.
Town Hall		
Applications to hire	7 years	VAT
Lettings diary		
Copies of invoices to hirers		
Allotments		
Waiting list	Shorter	
Allocation list	Indefinite because it is current	Audit, Management
Ex-plot holders' details	2 years after giving up the plot	Because we might get a question up to 2 years after.
Cemetery		
Register of fees collected	7 years	Audit
Register of burials	Indefinite	
Register of purchased graves	Indefinite (as long as they have the plot/memorial/etc, plus 6 years)	
Register/plan of grave spaces		
Register of memorials	Indefinite	
Notices of Interment		
Applications for the right to erect memorials.	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI 204)
Disposal Certificates	Indefinite	
Copy certificates of grant of Exclusive Right of Burial	5 years after the memorial has been erected.	
	Indefinite	
	Indefinite	

Sickness Absence Policy (11 pages) goes here but it will not copy due to embedded formats.

DRAFT