

STOKE ST MICHAEL PARISH COUNCIL

IT Policy

Approved by Full Council: -

1. Introduction

Stoke St Michael Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidance and responsibilities for the appropriate use of IT resources and email by the council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use Stoke St Michael Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Stoke St Michael Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All uses must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Stoke St Michael Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Stoke St Michael Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

6. Network and internet usage

Stoke St Michael Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Stoke St Michael Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Stoke St Michael Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote work

Mobile devices provided by Stoke St Michael Parish Council should be secured with passcodes and / or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Stoke St Michael Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

13. Training and awareness

Stoke St Michael Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

14. Policy Review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

15. Contacts

For IT-related enquiries or assistance, users can contact SoVision.

All staff and Councillors are responsible for the safety and security of Stoke St Michael Parish Council's IT and email systems. By adhering to this IT and Email policy, Stoke St Michael Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Stoke St Michael Parish Council

Bring Your Own Device Policy

Approved by Full Council: -

Introduction

Stoke St Michael Parish Council permits Councillors the use of their own smartphones and tablets of their choosing for council business.

This policy is intended to protect the security and integrity of personal data controlled and processed by Stoke St Michael Parish Council.

Stoke St Michael Parish Council reserves the right to revoke this permission if Councillors and Officers do not abide by the policies and procedures outlined below.

Stoke St Michael Parish Council Councillors must agree to the terms and conditions set forth in this Bring Your Own Device policy to receive and process Council data on their device.

Stoke St Michael Parish Council officers are provided with digital devices solely for the purposes of their work. Use of private devices for processing council data and work is not permitted. **To note** that the Parish Council does not own a Parish Council laptop, the Parish Council may need to consider purchasing one.

Devices and Support

- Smartphones, Tablets and Laptops are permitted at meetings.
- The device manufacturer or their carrier should be contacted for operating system or hardware related issues.

Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the council network.
- Passwords must be at least six characters and a combination of upper and lower-case letters with at least one number and one symbol.
- Passwords must be kept confidential and must not be shared with family members or third parties.
- Passwords must be changed if it is disclosed to another person or discovered.
- Devices must be encrypted.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Home Wi-Fi must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
- Public data backup and transfers services (e.g. Dropbox, Google Drive) must not be used.
- Data must only be stored on internal memory, never on a removable memory card.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- All data relating to Stoke St Michael Parish Council will be erased at the end of a Councillor's term or in the case of an Officer at the end of his or her employment.
- All data relating to Stoke St Michael Parish Council will be erased if there is a personal data breach.
- All data related to Stoke St Michael Parish Council will be erased if there is a virus or similar threat to the security of data.

- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or otherwise. Some apps for smartphones and tablets may be capable of accessing sensitive information.
- Councillors and officers will undertake regular training as relevant in relation to identifying phishing attacks, spam etc.

Risks / Liabilities / Disclaimers

- Councillors are responsible for notifying their mobile carrier immediately upon loss of a device.
- Councillors (and officers) to adhere to the Stoke St Michael Parish Council's Bring Your Own Device policy as outlined above.
- Councillors and Officers are personally liable for all costs associated with their device.
- Stoke St Michael Parish Council reserves the right to take appropriate disciplinary action (up to and including termination of employment for officers) for noncompliance with this policy.

STOKE ST MICHAEL PARISH COUNCIL
FREEDOM OF INFORMATION POLICY

Approved –

Introduction

Stoke St Michael Parish Council (the "Council") is committed to transparency and accountability. This Freedom of Information (FOI) Policy sets out how the Council will comply with its obligations under the Freedom of Information Act 2000 (FOIA) and relevant local government legislation. The FOIA provides individuals with the right to request access to information held by public authorities, including Parish councils.

The aim of this policy is to ensure that the Parish Council provides a clear framework for handling FOI requests, including how information is made available, what exemptions may apply, and how requests will be processed within statutory timescales.

Scope of the Policy

This policy applies to all recorded information held by the Parish Council, regardless of format. This includes information held in emails, minutes, reports, letters, electronic files, or any other form.

Under the FOIA, the Parish Council is obliged to:

- Confirm or deny whether it holds the information requested (subject to exemptions).
- Supply the requested information (subject to exemptions), where it is held and where it is not subject to limitations or prohibitive costs.

Legislation

The key legislation underpinning this policy includes:

- Freedom of Information Act 2000: Grants public access to information held by public authorities.
- Environmental Information Regulations 2004 (EIR): Relates to requests for environmental information.
- Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR): Governs the processing of personal data and works alongside the FOIA where requests involve personal data.
- Local Government Act 1972: Sets out the statutory framework for how public information is published, particularly relating to Parish Council minutes, agendas, and reports.

The Publication Scheme

Under Section 19 of the FOIA, the Parish Council is required to maintain and regularly update a Publication Scheme. The scheme outlines the types of information that the Parish Council routinely makes available to the public and how that information can be accessed. The scheme categorises information into the following areas:

- Who we are and what we do: Information about the Parish Council, its members, and its governance.
- What we spend and how we spend it: Financial statements, budgets, audit reports, and details of contracts.
- What our priorities are and how we are doing: Strategic plans, performance reports, and service reviews.
- How we make decisions: Decision-making processes, meeting agendas, minutes, and reports.
- Our policies and procedures: The Parish Council's policies, procedures, and guidelines.
- Lists and registers: Any statutory registers or records the Parish Council is required to maintain.
- Services we offer: Information about the services the Council provides.

The Publication Scheme is available on the Parish Council's website or upon request from the Parish Office. Where information is available online, a direct link will be provided.

Making a Request

Anyone can make a FOI request to the Parish Council. Requests must:

- Be made in writing (this includes email).
- Provide the name of the applicant and a contact address.
- Clearly describe the information being sought.

The Parish Council may ask for further clarification if the request is unclear or too broad. Requests should be sent to:

Proper Officer to the Council
Stoke St Michael Parish Council
Uphill Cottage
Church Street
Croscombe
Somerset
BA5 3QS
Email: clerk@stokestmichaelpc.org

Processing Requests

Upon receiving a valid FOI request, the Council will:

1. Acknowledge the Request: The Parish Council will acknowledge receipt of the request in writing within 5 working days.
2. Timeframe for Response: The Parish Council is required to respond to the FOI request within 20 working days from the date of receipt. If an extension is required due to complexity, the applicant will be informed.
3. Confirmation: The Parish Council will confirm or deny whether it holds the requested information, subject to any applicable exemptions.
4. Providing the Information: Where the information is held and no exemptions apply, the Parish Council will provide the requested information in the preferred format, where reasonable.
5. Fees: In accordance with Section 12 of the FOIA, the Parish Council may charge a fee if the cost of fulfilling the request exceeds the statutory cost limit. If this is the case, the applicant will be informed, and they may choose to refine their request to reduce costs.

Exemptions

Under the FOIA, certain information is exempt from disclosure. The Parish Council will apply exemptions where appropriate, as outlined in Part II of the FOIA, including but not limited to:

- **Personal Data:** Information covered by the Data Protection Act 2018 and UK GDPR.
- **Confidentiality:** Information provided in confidence, including correspondence between the Council and its legal advisors.
- **Commercially Sensitive Information:** Information that could harm the Council's commercial interests or that of third parties.
- **Law Enforcement:** Information that could prejudice law enforcement or legal proceedings.

If an exemption applies, the Parish Council will issue a Refusal Notice within 20 working days explaining why the information cannot be disclosed, citing the relevant section of the FOIA.

Vexatious and Repeated Requests

Under Section 14 of the FOIA, the Parish Council is not obliged to comply with vexatious or repeated requests. A request may be deemed vexatious if it is designed to cause disruption, is abusive, or imposes an unreasonable burden on the Council's resources.

If the Parish Council deems a request to be vexatious, it will issue a Refusal Notice explaining its decision. Guidance from the Information Commissioner's Office (ICO) will be followed to determine when a request is considered vexatious or unreasonable.

Charges and Fees

The Parish Council may charge a fee for responding to FOI requests that exceed the appropriate cost limit, as specified in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004. The appropriate limit is currently set at £450, which is equivalent to 18 hours of work at £25 per hour.

If the cost of complying with a request exceeds this limit, the Council will inform the applicant, offering them the opportunity to refine their request to reduce the cost. Where applicable, charges for photocopying, printing, and postage will be communicated to the applicant in advance.

Complaints and Internal Review

If an applicant is dissatisfied with the handling of their FOI request, they may request an internal review. Complaints should be directed to the Proper Officer to the Parish Council at the address provided under making a request. An internal review will be conducted, and a response will be provided within 20 working days.

If the applicant remains dissatisfied after the internal review, they may escalate the complaint to the Information Commissioner's Office (ICO) at:

Information Commissioners' Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Tel: 0303 123 1113

Website: <https://ico.org.uk/>

Telephone Helpline: 0303 123 1113

Stoke St Michael Parish Council

Internal Control Policy

Approved by Full Council: -

1. Scope of Responsibility

Stoke St Michael Parish Council (the Council) is responsible for ensuring that its business is conducted in accordance with the law and proper standards and that public money is safeguarded and properly accounted for and used economically, efficiently, and effectively.

In discharging this overall responsibility, the Council is also responsible for ensuring that there is a sound system of internal control, which facilitates the effective exercise of the Council's functions and includes arrangements for the management of risk.

2. The Purpose of the System of Internal Control

The system of internal control is designed to manage risk; reducing it to a reasonable level rather than to eliminate all risk of failure to achieve policies, aims and objectives. It can therefore only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an on-going process designed to identify and prioritise the risks to the achievement of the Council's policies, aims and objectives, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively, and economically.

3. The Internal Control Environment

3.1 The Council

The Council has appointed a chair who is responsible for the smooth running of its meetings. The Council reviews its obligations and objectives and budgets at the level of precept required for the following year at its January meeting. The Council monitors progress against its aims and objectives at its meetings by receiving relevant reports from the Parish Clerk. The Council regularly reviews its internal controls, systems, and procedures.

3.2 The Clerk / Responsible Financial Officer

The Council has appointed a Clerk and a Responsible Finance Officer (RFO). The Clerk of the Council acts as the Council's advisor and administrator. The Responsible Financial Officer is responsible for administering the Council's finances. The Clerk is responsible for the day-to-day compliance with laws, and regulations that the Council is subject to and for managing risks. The Clerk also ensures that the Council's procedures, control systems and policies are adhered to.

3.3 Payments – all payments are approved by the Council.

Two member signatories are required to sign every cheque. All electronic and direct debit payments (including debit card transactions) are subject to approval by two members (from the authorised list of Councillors with bank approval) which may be by means of the email approval of a periodic schedule of payments.

3.4 Risk Assessments / Risk Management

The Council carries out regular risk assessments in respect of its activities and regularly reviews its systems and controls.

3.5 Internal Audit

The Council has appointed an independent, competent internal auditor who reports to the Council on the adequacy of its systems, and procedures, internal controls and risk management and its reviews of these matters. The effectiveness of internal audit is reviewed annually.

3.6 External Audit

The Council's external auditors submit an annual certificate of Audit which is presented to the Council.

4. Review of Effectiveness

The Council has responsibility for conducting an annual review of the effectiveness of the system of internal control. The review of the effectiveness of the system of internal control is informed by the work of:

- The Council
- The Clerk / FO who has responsibility for the design and maintenance of the internal control environment and managing risk.
- The independent internal auditor who reviews the Council's systems of internal control.
- The Council's external auditor who makes the final check using the annual return, a form completed and signed by the Clerk / RFO, the Chairman and internal auditor.

5. Significant Internal Control Issues

The Council strives for the continuous improvement of the system it has designed for internal control and has addressed all of the minor issues and weaknesses raised and reported during the review process.

Statement of Internal Control

Cash Book / Bank Reconciliations

The cash book is kept electronically on a spreadsheet (Excel) and kept up to date from the original documents – receipts, invoices, and bank statements. The cash book is reconciled to the bank statement each month and a bank reconciliation is approved quarter at the Parish Council meeting. The bank statements are checked against the bank reconciliation by a member of the council.

The bank reconciliation shall include all bank accounts (current, savings, deposit and other accounts) held by the council and shall show movements of balances on all accounts.

Financial Regulations

The Parish Council has adopted Financial Regulations based on the NALC model. The regulations are reviewed for continued relevant and amended where necessary via approval by the Parish Council.

Order / Tender Control

Financial Regulations refer to procedures relating to tenders.

Legal Power

A proper legal power is identified for each expenditure.

Payment Controls

Two member signatories are required to sign every cheque. All electronic and direct debit payments (including debit card transactions) are subject to approval by two members (from the authorised list of Councillors with bank approval) which maybe by means of the email approval of a periodic schedule of payments.

All payments are reported to the Council for approval via a schedule of payments and receipts, this is done at each Parish Council Meeting.

The RFO maintains control of the cheque book and debit card which are kept in a secure place.

VAT Reclaims

The RFO ensures that all invoices are addressed to the Parish Council. The RFO maintains a VAT account and ensures that the correct amount of VAT is reclaimed in the year and in the required time frames.

Income Controls

All income is received and banked in the Council's name in a timely manner and reported to the Council. The Parish Clerk ensures that the amount of precept received is correct in accordance with the precept request sent to Somerset Council and ensures that the precept instalments are received when due.

Financial Reporting

A budget control, comparing actual receipts and payments to the budget is prepared and presented to the Council quarterly.

Budgetary Controls

The budget is prepared in consultation with the Councillors at the October / November meeting and the level of precept is approved by the full Council at the January meeting each year. The precept request is submitted by the deadline dictated by Somerset Council.

Payroll Controls

All employees are under PAYE as an employee of the Council and the necessary system for making payments to HMRC is in place.

The payroll included amounts payable to HMRC.

In April each year the Annual Gross pay, Employers National Insurance and Employers Pension contributions are checked against Employees remuneration as per their contracted terms and conditions.

Risk Assessment

Risk Assessment for the Parish Council is presented annually to the Parish Council for review and approval.

Asset Control

The Clerk maintains a full asset register. The existence and conditions of assets is checked on an annual basis by the Parish Council. The adequacy of insurance of the Parish Council's assets is considered annually in advance of the insurance renewal. The insurance schedule is checked annually before being renewed.

Internal Audit

The Council annually appoints an independent internal auditor who provides a full report to the Council. The internal auditor will have planned and carried out the work necessary to give the assurances called for in section 4 of the Local Councils Annual Return. The Parish Council reviews the scope of work offered by the Internal Auditor.

External Audit

The Council submits an annual return to the external auditor in a timely manner.

Policy and Decision Making

The facilitation of policy and decision-making is through the full Council. Committees function within approved Terms of Reference that are reviewed annually. Meetings are open to the public except where personal or confidential matters are being discussed in accordance with the relevant legislation.

STOKE ST MICHAEL PARISH COUNCIL

PRIVACY POLICY (GDPR)

Approved –

This Policy has been adopted by Stoke St Michael Parish Council in order to comply with the requirements of the General Data Protection Regulations (GDPR).

Data Processing is any activity that involves the use of personal data. Processing also includes transmitting or transferring personal data to third parties.

Personal Data is any information about a living individual, which allows them to be identified from that data (for example, a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the “GDPR”).

This Privacy Policy is provided to you by Stoke St Michael Parish Council which is the data controller for your data.

When you contact us

The information you provide (personal information such as name, address, email address, phone number, organisation) will be processed and stored to enable us to contact you and respond to your correspondence, provide information and/or access our facilities and services. Your personal information will be not shared or provided to any other third party.

The Councils Right to Process Information

General Data Protection Regulations Article 6 (1) (a) (b) and (e)

Processing is with consent of the data subject or

Processing is necessary for compliance with a legal obligation or

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Information Security

Stoke St Michael Parish Council has a duty to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction, or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. Copies of these policies can be requested.

We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted. (You may request the deletion of your data held by Stoke St Michael Parish Council at any time).

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Access to Information

You have the right to request access to the information we have on you. You can do this by contacting our Data Information Officer: Stoke St Michael Parish Council

Information Correction

If you believe that the information, we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: Stoke St Michael Parish Council to request this.

Information Deletion

If you wish Stoke St Michael Parish Council to delete the information about you, please contact: Stoke St Michael Parish Council to request this.

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact Stoke St Michael Parish Council to object.

Rights Related to Automated Decision Making and Profiling

Stoke St Michael Parish Council does not use any form of automated decision making or the profiling of individual personal data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to: Stoke St Michael Parish Council, Data Information Officer, Town Hall, The Island, Midsomer Norton BA3 2HA and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

Summary: In accordance with the law Stoke St Michael Parish Council only collect a limited amount of information about you that is necessary for correspondence, information, and service provision. Stoke St Michael Parish Council do not use profiling; we do not sell or pass your data to third parties. Stoke St Michael Parish Council do not use your data for purposes other than those specified. Stoke St Michael Parish Council make sure your data is stored securely. Stoke St Michael Parish Council delete all information deemed to be no longer necessary. Stoke St Michael Parish Council constantly review our Privacy Policies to keep it up to date in protecting your data. (You can request a copy of our policies at any time).

STOKE ST MICHAEL PARISH COUNCIL

PUBLICATION SCHEME

Approved –

Reviewed

Model Publication Scheme

Freedom of Information Act

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.

Classes of Information

Who we are and what we do?

Organisational information, location and contacts, constitutional and legal governance

What we spend and how we spend it?

Financial information relating to projected and actual income and expenditure, tendering, procurement, and contracts.

What our priorities are and how we are doing

Strategy and performance information, plans, assessments, inspections, and reviews.

How we make decisions

Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.

Current written protocols for delivering our functions and responsibilities.

List and registers.

Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.

Advice and guidance, booklets and leaflets, transactions, and media requests. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information on draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available.

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme.

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.

Charges may be made for information. Charges may be made for actual disbursements incurred such as:

- Photocopying
- Postage and packaging
- The costs directly incurred as a result of viewing information.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Photocopying – 50p per A4 sheet (Black and white)

Postage – Actual cost of Royal Mail standard 2nd class

Written Requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.

Information available from Stoke St Michael Parish Council under the model publication scheme

This scheme commits the Council to make information available to the public as part of its normal business activities. The information is included in the classes of information outlined below.

Where possible information will be provided on the Council's website but where it is impractical, hard copies of some information can be made available. The policy below states how information can be obtained.

In exceptional circumstances some information may be available only by viewing in person. An appointment to view the information can be arranged within a reasonable timescale.

Information held by the Parish Council that is not published under this Scheme can be requested in writing, when its provision will be considered in accordance with the Freedom of Information Act.

Information in this definition document will be made available unless

- The information is no longer held.
- The information is exempt under one of the FOIA exemptions or its release is prohibited by another statute.
- The information is readily and publicly available from an external website; such information may have been provided by the public authority or on its behalf. The authority must provide a direct link to that information.
- The information is archived, out of date or otherwise inaccessible.
- It would be impractical or resource-intensive to prepare the material for routine release.

Information published	How the information can be obtained
Class 1 – Who we are and what we do?	
Organisational information, structures, locations, and contracts. Current information only.	
Who's who on the Council and its Committees	Website or hard copy
Contact Details for Parish Clerk and Council Members Named contacts with email addresses.	Website or hard copy
Location of main Council office and accessibility details	Website or Hard Copy
Staffing Structure	Website or Hard Copy
Class 2 – What we spend and how we spend it?	
Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit. Current and previous year as a minimum	
Annual return form and report by auditor	Website or hard copy
Finalised budget	Website or hard copy
Precept	Website or Hard Copy
Financial Standing Orders and Regulations	Website or Hard Copy
Grants given and received, included with appropriate minutes	Website or Hard Copy
List of current contracts awarded and value of contract	Website or Hard Copy
Members' allowances and expenses	Hard Copy
Class 3 – What our priorities are and how we are doing?	
Strategies and plans, performance indicators, inspections and reviews	
Parish Plan	N/A
Village Design Statement	Website or Hard Copy
Neighbourhood Development Plan	N/A
Annual Report to Parish or Community Meeting	Website or hard copy
Class 4 – How we make decisions?	
Decision making processes and records of decisions. Current and previous year as a minimum	
Timetable of meetings (Council and any committee / sub-committee and Parish Meetings)	Website or hard copy
Agendas of Meetings	Website, hard copy and Notice Board
Minutes of Meetings	Website or hard copy
Reports presented to council meetings	Website or hard Copy
Responses to consultation paper	Hard Copy
Responses to Planning Applications	Somerset Council Website and Hard Copy

Class 5 – Our policies and procedures Current written protocols, policies and procedures for delivering our services and responsibilities. Current information only.	
Policies and procedures for the conduct of council business: Including Standing Orders detailing delegated authority, Financial Regulations, Code of Conduct and other Policy statements	Website or hard copy
Policies and procedures for the provision of services and about the employment of staff: Including Equality and Diversity Policy, Health and Safety Policy, Recruitment Policies, Policies and procedures for handling requests for information, Complaints procedures (including those requests for information and operating the publication scheme).	Website or hard copy
Records management policies (records retention, destruction and archive)	Website or hard copy
Data Protection Policies	Website or hard copy
Schedule of charges for requests for information	Contained in this policy
Class 6 – List and Registers Currently maintained lists and registers only	
Any publicly available register or list, if any are held should be publicised	Website or hard copy
Assets Register	Website or Hard Copy
Disclosure log (indicating the information that has been provided in response to requests, recommended as good practice)	Website or Hard Copy
Register of Members Interests	Website or Hard Copy
Register of gifts and hospitality	Website or Hard Copy
Class 7 – The services we offer. Information about the services we offer including leaflets, guidance and newsletters produced for the public and businesses. Current information only	
Cemetery	Website or Hard Copy
Seating, Litter Bins, Memorials and Lighting	Hard Copy
Bus Shelters	Hard Copy
Parks, playing fields and recreational facilities	Hard Copy
A summary of services for which the council is entitled to recover a fee, together with those fees	Hard Copy

Additional Information	
This will provide Councils with the opportunity to publish information that is not itemised in the lists above	
Declarations of acceptance of office	Hard Copy
Newsletter	Website or Hard Copy

Contact Details

Parish Clerk: Parish Clerk
 Stoke St Michael Parish Council
 Uphill Cottage
 Church Street
 Croscombe
 Somerset
 BA5 3QS

STOKE ST MICHAEL PARISH COUNCIL

RETENTION AND DISPOSAL POLICY

Adopted: -

To Be Reviewed: -

1. Introduction

- 1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of documents.
- 1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.
- 1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.
- 1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage, and difficulty in defending any claim brought against the Council.
- 1.5 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

2. Scope and Objectives of the Policy

- 2.1 The aim of this document is to provide a working framework to determine which documents are:
- Retained – and for how long; or
 - Disposed of – and if so by what method.
- 2.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:
- 'With compliments' slips.
 - Catalogues and trade journals.
 - Non-acceptance of invitations.
 - Trivial electronic mail messages that are not related to Council business.
 - Requests for information such as maps, plans or advertising material.
 - Out of date distribution lists.
- 2.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.

- 24 Records should not be destroyed if the information can be used as evidence. to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulation.

3. Roles and Responsibilities for Document Retention and Disposal

- 3.1 Councils are responsible for determining whether to retain or dispose of documents and should undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the General Data Protection Regulations.
- 3.2 Councils should ensure that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

- 4.1 Councils should have in place an adequate system for documenting the activities of their service. This system should consider the legislative and regulatory environments to which they work.
- 4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:
- Facilitate an audit or examination of the business by anyone so authorised.
 - Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
 - Verify individual consent to record, manage and record disposal of their personal data.
 - Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.
- 4.3 To facilitate this the following principles should be adopted:
- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations
 - Documents that are no longer required for operational purposes but need retaining should be placed at the records office.
- 4.4 The retention schedules in Appendix A: List of Documents for Retention or Disposal provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.
- 4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

5. Document Disposal Protocol

- 5.1 Documents should only be disposed of if reviewed in accordance with the following:
- Is retention required to fulfil statutory or other regulatory requirements?
 - Is retention required to meet the operational needs of the service? Is retention required to evidence events in the case of dispute?
 - Is retention required because the document or record is of historic interest or intrinsic value?
- 52 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept complying with the General Data Protection Regulations.
- 53 Documents can be disposed of by any of the following methods:
- Non-confidential records: place in wastepaper bin for disposal.
 - Confidential records or records giving personal information: shred documents.
 - Deletion of computer records.
 - Transmission of records to an external body such as the County Records Office.
- 54 The following principles should be followed when disposing of records:
- All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.
 - the Freedom of Information Act or cause reputational damage.
 - Where computer records are deleted, steps should be taken to ensure that data is 'Virtually impossible to retrieve' as advised by the Information Commissioner.
 - Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.
 - Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).
- 55 Records should be maintained of appropriate disposals. These records should contain the following information:
- The name of the document destroyed.
 - The date the document was destroyed.
 - The method of disposal.

6. Data Protection Act 2018 – Obligation to Dispose of Certain Data

- 6.1 The Data Protection Act 2018 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:

Data that relates to a living individual who can be identified:

- a) from the data, or
- b) from those data and other information, which is in the possession of, or is likely to come into the possession of the data controller.

It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.

- 6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met.
- 6.3 Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations namely:
- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met. Personal data shall only be obtained for specific purposes and processed in a compatible manner.
 - Personal data shall be adequate, relevant, but not excessive.
 - Personal data shall be accurate and up to date.
 - Personal data shall not be kept for longer than is necessary.
 - Personal data shall be processed in accordance with the rights of the data subject.
 - Personal data shall be kept secure.
- 6.4 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

7. Scanning of Documents

- 7.1 In general, once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.
- 7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.
- 7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

8. Review of Document Retention

- 8.1 It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the *Code of Practice on the Management of Records* issued by the Lord Chancellor).
- 8.2 This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:
- *Local Council Administration*, Charles Arnold-Baker, 12th edition, Chapter 11
 - NALC LTN 40 – *Local Councils' Documents and Records*, January 2013
 - NALC LTN 37 – *Freedom of Information*, July 2009
 - *Lord Chancellor's Code of Practice on the Management of Records* issued under Section 46 of the *Freedom of Information Act 2000*

STOKE ST MICHAEL PARISH COUNCIL
LIST OF DOCUMENTS FOR RETENTION OR DISPOSAL

Adopted: -

To Be Reviewed: -

Document	Minimum Retention Period	Reason	Disposal
Minutes	Indefinite	Archive	Original signed paper copies of Council minutes of meetings must be kept indefinitely in safe storage. At regular intervals of not more than 5 years they must be archived and deposited with the Higher Authority
Agendas	5 years	Management	Bin (shred confidential waste)
Accident/incident reports	20 years	Potential claims	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Scales of fees and charges	6 years	Management	Bin
Receipt and payment accounts	Indefinite	Archive	N/A
Receipt books of all kinds	6 years	VAT	Bin
Bank statements including deposit/savings accounts	Last completed audit year	Audit	Confidential waste
Bank paying-in books	Last completed audit year	Audit	Confidential waste
Cheque book stubs	Last completed audit year	Audit	Confidential waste
Quotations and tenders	6 years	Limitation Act 1980 (as amended)	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Paid invoices	6 years	VAT	Confidential waste
Paid cheques	6 years	Limitation Act 1980 (as amended)	Confidential waste
VAT records	6 years generally but 20 years for VAT on rents	VAT	Confidential waste
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	Confidential waste

Document	Minimum Retention Period	Reason	Disposal
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)	Bin
Wages books/payroll	12 years	Superannuation	Confidential waste
Insurance policies	While valid (but see next two items below)	Management	Bin
Insurance company names and policy numbers	Indefinite	Management	N/A
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	Bin
Town Park equipment inspection reports	21 years	Audit, Management	Confidential waste
Investments	Indefinite	Audit, Management	N/A
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	N/A
Members' allowances register	6 years	Tax, Limitation Act 1980 (as amended)	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Information from other bodies e.g. circulars from county associations, NALC, principal authorities	Retained for as long as it is useful and relevant		Bin

Document	Minimum Retention Period	Reason	Disposal
Local/historical information	Indefinite – to be securely kept for benefit of the Parish	Councils may acquire records of local interest and accept gifts or records of general and local interest in order to promote the use for such records (defined as materials in written or other form setting out facts or events or otherwise recording information).	N/A
Magazines and journals	<p>Council may wish to keep its own publications.</p> <p>For others retain for as long as they are useful and relevant.</p>	The Legal Deposit Libraries Act 2003 (the 2003 Act) requires a local council which after 1 st February 2004 has published works in print (this includes a pamphlet, magazine or newspaper, a map, plan, chart or table) to deliver, at its own expense, a copy of them to the British Library Board (which manages and controls the British Library). Printed works as defined by the 2003 Act published by a local council therefore constitute materials which the British Library holds.	Bin if applicable

Document	Minimum Retention Period	Reason	Disposal
Record Keeping			
<p>To ensure records are easily accessible it is necessary to comply with the following:</p> <ul style="list-style-type: none"> • A list of files stored in cabinets will be kept. • Electronic files will be saved using relevant file names. 	<p>The electronic files will be backed up periodically on a portable hard drive and also in the cloud-based programme supplied by the Council's IT company.</p>	<p>Management</p>	<p>Documentation no longer required will be disposed of, ensuring any confidential documents are destroyed as confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</p>
<p>General correspondence</p>	<p>Unless it relates to specific categories outlined in the policy, correspondence, both paper and electronic, should be kept. Records should be kept for as long as they are needed for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.</p>	<p>Management</p>	<p>Bin (shred confidential waste) A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</p>

Document	Minimum Retention Period	Reason	Disposal
Correspondence relating to staff.	If related to Audit, see relevant sections above. Should be kept securely and personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. Likely time limits for tribunal claims between 3–6 months. Recommend this period be for 3 years.	After an employment relationship has ended, a council may need to retain and access staff records for former staff for the purpose of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the council.	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Documents from legal matters, negligence, and other torts Most legal proceedings are governed by the Limitation Act 1980(as amended). The 1980 Act provides that legal claims may not be commenced after a specified period. Where the limitation periods are longer than other periods specified the documentation should be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories. If in doubt, keep for the longest of the three limitation periods.			
Negligence	6 years		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Defamation	1 year		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Contract	6 years		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Leases	12 years		Confidential waste.
Sums recoverable by statute	6 years		Confidential waste.
Personal injury	3 years		Confidential waste.
To recover land	12 years		Confidential waste.

Document	Minimum Retention Period	Reason	Disposal
Rent	6 years		Confidential waste.
Breach of trust	None		Confidential waste.
Trust deeds	Indefinite		N/A
For Halls, Centres, Recreation Grounds			
<ul style="list-style-type: none"> • Application to hire. • Invoices • Record of tickets issued 	6 years	VAT	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Lettings diaries	Electronic files linked to accounts	VAT	N/A
Terms and Conditions	6 years	Management	Bin
Event Monitoring Forms	6 years unless required for claims, insurance or legal purposes	Management	Bin. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
For Allotments			
Register and plans	Indefinite	Audit, Management	N/A
Minutes	Indefinite	Audit, Management	N/A
Legal papers	Indefinite	Audit, Management	N/A
For Burial Grounds			
<ul style="list-style-type: none"> • Register of fees collected • Register of burials • Register of purchased graves • Register/plan of grave spaces • Register of memorials • Applications for interment • Applications for right to erect memorials • Disposal certificates • Copy certificates of grant of exclusive right of burial 	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI 204)	N/A

Document	Minimum Retention Period	Reason	Disposal
For Planning Papers			
Applications	1 year	Management	Bin
Appeals	1 year unless significant development	Management	Bin
Trees	1 year	Management	Bin
Document	Minimum Retention Period	Reason	Disposal
Local Development Plans	Retained as long as in force	Reference	Bin
Local Plans	Retained as long as in force	Reference	Bin
Town/Neighbourhood Plans	Indefinite – final adopted plans	Historical purposes	N/A
For CCTV			
Daily notes	Daily	Data protection	Confidential waste
Radio rotas	1 week	Management	Confidential waste
Work rotas	1 month	Management	Confidential waste
Observation sheets	3 years	Data protection	Confidential waste
Stats	3 years	Data protection	Confidential waste
Signing in sheets	3 years	Management	Confidential waste
Review requests	3 years	Data protection	Confidential waste
Discs – master and working	For as long as required	Data protection	Confidential waste
Internal Operations Procedure Manual	Destroy on renewal. Review annually	Management	Confidential waste
Code of Practice	Destroy on renewal. Review annually	Management	Confidential waste
Photographs/digital prints	31 days	Data protection	Confidential waste

General Data Protection Regulation (GDPR)

Produced July 2025

PERSONAL DATA AUDIT QUESTIONNAIRE

- A. To be used to help Councils with their record keeping obligations under the GDPR.
- B. This questionnaire is designed to help Councils to audit their personal data. It is important that Councillors and staff complete this form as comprehensively as possible. The purpose of a data audit is to find out what data the Council is processing, what it is used for, where it is located and, who has access to it. It is an important step in assessing whether there are any risks in the type of processing the Council carries out. For example, if the Council processes a large amount of sensitive personal data but has no access controls in place restricting who can see or use the data, that is a security risk which needs to be fixed. Without carrying out an audit a Council may not know what risks it currently has with data.
- C. The generic phrase 'Council' has been used to refer to the data controller (see glossary) using the questionnaire.

D. Glossary

'Personal Data' is any information about a living person which can identify them. This is not just someone's name and address but any information which can identify them (directly or indirectly). For example, a phone number or email address is personal data. Any other contact information or a person's employment history, or credit history are all personal data.

'Data Controller' is the person or organisation who determines the how and what of data processing.

'Data processor' is the person or firm that processes the data on behalf of the controller.

'Data subject' is the person about whom personal data is processed.

'Processing' personal data means storing or deleting any personal data on a computer, database, or some manual files (e.g. HR, allotment tenancy files or invoices with contractor payment details). The word 'processing' also cover selecting a name for a mailing list or reading it off a screen during a call. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing.

'Sensitive personal data or special categories or personal data' are any of the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

PART A: YOUR INFORMATION

1. Person completing questionnaire.

Name	Kate Egan
Role	Parish Clerk
Telephone number	01749 343910
Email	clerk@stokestmichaelpc.org

2. Data Controller (Name of Local Council) Stoke St Michael Parish Council

3. Date you completed this questionnaire 31st July 2025

PART B: COMMUNICATING PERSONAL DATA relates to communications with councillors, staff, and local residents (including mailing list), general public.

4. What type of personal data does the Council keep? e.g. name, contact details such as bank details.

Name, Address, Telephone Number(s), Email, Address, Financial Information, Bank Details, Staff NI Number(s), Payroll Records, Photographs.

5. Where does the Council get the personal data from? e.g. staff, residents, other local authorities, charities and sports clubs, community groups, recruitment agencies.

Staff, Councillors, Other Local Authorities, Residents, General Public, Charities, Sports Clubs, Community Groups, Contractors, Businesses, Volunteers

6. Why does the Council collect or process the data – what does the Council do with the personal data? For purposes relating to e.g. local resident concerns, management of Council facilities, services and staff, contract management, performance of statutory functions. *(Please list all reasons).*

Local Resident Concerns – Gmail, correspondence folder

Management of Council facilities – Gmail, leaflets, laptop, website (held for statutory purposes and to advertise facilities).

Services – Gmail, contract folder, correspondence folder, laptop, website, online banking (held for contractual purposes and payments)

Staff – Gmail, HMRC Payroll software, laptop, website, online banking (held for transparency purposes, salaries, and payments)

Councillors – Gmail, laptop, website, online banking (held for transparency purposes and expenses payments)

Contract Management – Gmail, contract folder, correspondence folder, laptop, website, online banking (held for contractual purposes and payments)

Performance of Statutory Functions – Gmail, correspondence folder, laptop, website, online banking (held for contractual purposes and payments)

- 7. Who does the Council disclose personal data to?** E.g. the public, Councillors, staff and contractors carrying out the work of the Council, pension providers, HMRC, credit reference agencies, recruitment agencies, prospective employers.

Public, Councillors, Staff, Contractors, Pension Provider, HMRC

- 8. Do the Council minutes contain personal data?**

No; the press and public are excluded from the meeting when confidential and commercially sensitive matters are discussed, and information is not available for public inspection thereafter. Members of the public are not mentioned during the public session.

- 9. Does the Council ever send personal data overseas and if so where to and which organisation? This might include overseas companies providing database or email services.** E.g. Do any of your suppliers use 'cloud storage' and if so, do you know where the personal data is located?

Only to the general public who reside overseas and have made an enquiry by email or are able to view the website.

- 10. Does the Council collect any sensitive personal data?** See definition above.

Yes.

- 11. If so for what reason?** E.g. for safeguarding compliance; physical or mental health data relating to staff; racial and ethnic origin relating to equal opportunities monitoring. (Please list anything else)

Current staff personal data is held for three years following departure from the Council. Councillor information is retained until the next ordinary election.

PART C: SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS THE COUNCIL CONTRACTS WITH

about individuals or representatives of organisations which supply us with services such as for council repairs, or with whom we are in contact.

- 12. Who does the Council keep personal data about?** e.g. tradesmen, recruitment agencies, surveyors, architects, builders, suppliers, advisors, payroll processor. (Please list any others)

Contractors, businesses, solicitors, suppliers of goods and services, service providers, volunteers

- 13. What type of personal data does the Council keep?** e.g. name, contact details, qualifications, financial details, details of certificates and diplomas, education and skills. (Please list any others).

Name, address, email, telephone number(s), PLI schedules (if applicable), risk assessments (if applicable), method statements (if applicable), staff employment documents including qualifications and CV.

14. Where does the Council get the data from? e.g. the individuals, suppliers. (Please list any others).

Individuals, businesses, goods providers, service providers.

15. Why does the Council collect or process the data? e.g. Council property maintenance and repairs and management of Council facilities, pay and manage staff. (Please list any other reasons).

Maintenance and repairs contracts, goods and services, legal matters, payment for good / services, tenants leasing or renting land, service agreements.

PART D: GENERAL QUESTIONS ABOUT PERSONAL DATA

16. How does the Council store the personal data collected?

Clerks home office, laptop, website, memory stick, outlook, folders

17. Does the Council take any steps to prevent unauthorised use of access to personal data or against accidental loss, destruction, or damage? If so, what?

Archived information is stored at the County Archives in Taunton. Some current information is stored at the Clerk's home address. Insurance cover is in place for indemnity but there are no possible methods to safeguard against accidental loss, destruction, damage, or theft.

18. How does the Council manage access to data?

The Clerk's home office is not accessible to members of the public or visitors and information at the Clerk's home is stored upstairs.

19. What is the process involved in giving access to staff or Councillors?

The Clerk is the only member of staff and Councillors are made aware of any confidential information which is not available for public inspection.

20. Do any procedures exist for e.g. correcting, deleting, restricting, personal data? If so, please provide details.

NALC Legal Topic 40 November 2016 Local Council's Documents and Records

21. Who has access to / is provided with the personal data (internally and externally)?

Clerks, Office Staff, Councillors, Contractors, other Local Authorities

22. Is there an authorisation procedure for accessing personal data? If so, please provide details.

The Council has a Privacy Policy

23. Does the Council provide a copy of all existing privacy notices?

The Privacy Notice is displayed on the website.

24. So far as the Council is aware, has any personal data which was gathered for one purpose been used for another purpose (e.g. communicating Council news?) If so, please provide details.

No

25. Does the Council have any policies, processes, or procedures to check the accuracy of personal data?

No

26. In the event of a data security breach occurring, does the Council have in place processes or procedures to be followed? What are these?

Personal Data Breaches policy to be adopted

27. If someone asks for a copy of personal data that the Council holds about them, i.e. they make a 'subject access request', is there a procedure for handling such a request? Is this procedure contained in a written document?

Subject Access Policy (SAR) to be adopted

28. Does the Council have an internal record of the consents which the Council has relied upon for processing activities? e.g. to send Council newsletters to residents.

Not applicable

29. Are cookies used on our Council Website?

Yes

30. Does the Council provide information about the cookies used and why they are used?

Yes

31. Does the Council keep a record of consents provided by users to the cookies?

No

32. Does the Council allow individuals to refuse to give consent?

Not applicable

33. Does the Council have website privacy notices and privacy policies?

Yes

34. What data protection training do staff and Councillors receive?

The Deputy Clerk has received training on GDPR and Data Protection

35. Does anyone in the Council have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date?

The Clerk, and the Chair.

36. What does the Council do about archive, retention, or deletion of personal data?

Archived information is stored at the Council Archives in Taunton. The Council follows the Retention and Disposal Policy.

37. How long is personal data kept before being destroyed or archived?

Obsolete emails are deleted and correspondence is shredded after 6 months from receipt. Information is only kept for as long as it is required.

PART E: MONITORING

38. Please identify any monitoring of the following systems that takes place.

‘Monitoring’ includes all monitoring of systems including intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are:

- Computer networks and connections
- CCTV and access control systems
- Communications systems (e.g. intercom, public address systems, radios, walkie-talkies)
- Remote access systems
- Email and instant messaging systems
- Telephones, voicemail, mobile phone records
- (Please list anything else)

The Clerk and Councillors are responsible for ensuring the items listed are kept up to date and information via communication systems are stored and / or deleted when necessary.

39. Does the Council have notices, policies, or procedures relevant to this monitoring?

Social Media Policy