Policy Group: General

Data Protection and Retention Policies

RESPONSIBLE COMMITTEE: P&F

This is a policy/procedure document of Saltash Town Council to be followed by both Councillors and Employees.

Current Document Status			
Version	2024/25	**Approved by**	ATM
Date	02.05.2024	**Responsible Officer**	AJT
Minute no.	64/24/25c(5)	**Next review date**	Annual or as required

Version History					
Date	**Version**	**Author/ editor**	**Committee/ date**	**Minute no.**	**Notes**
02.2024	1 DRAFT	AJT	P&F 27.02.2024	156/23/24c(5)	Combined policy document. For recommendation to FTC 03.2024.
03.2024	2024	AJT	FTC 07.03.2024	367/23/24c	Rec. from P&F. Approved
05.2024	2024	AJT	ATM 02.05.2024	64/24/25c(5)	Readopted

Document Retention Period
Until superseded

Contents

Data Retention and Disposal Policy

NOTE: This document refers to the now repealed Data Protection Act 1998 which has been replaced by the Data Protection Act 2018.

1. Introduction

1.1 The Town 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 document.

1.2 Records created and maintained by the Town 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 Town 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 Town 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 Town Council.

1.5 In contrast to the above the Town Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the UK 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 Town 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.

2.4 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 Regulations

3. Roles and Responsibilities for Document Retention and Disposal

3.1 The Town Council is 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 UK General Data Protection Regulations.

3.2 The Town Council should ensure that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

4.1 Town Councils should have in place an adequate system for documenting the activities of their service. This system should take into account 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 Town 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 UK 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?

5.2 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 to comply with the General Data Protection Regulations.

5.3 Documents can be disposed of by any of the following methods:

- Non-confidential records: place in waste paper 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.

5.4 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 Town Council being prosecuted under the UK 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).

5.5 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 1998 (REPEALED AND REPLACED BY THE Data Protection Act 2018 23rd May 2018)– Obligation to Dispose of Certain Data

6.1 The Data Protection Act 1998 ('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 Town 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 Town Councils are responsible for ensuring that they comply with the principles of the under the UK 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 Town 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 Town Council Administration*, Charles Arnold-Baker, 910^{h} edition, Chapter 11
- Local Government Act 1972, sections 225 – 229, section 234

- *SLCC Advice Note 316 Retaining Important Documents*
- *SLCC Town Clerks' Manual: Storing Books and Documents*
- *Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000*

9. List of Documents

9.1 The full list of the Town Council's documents and the procedures for retention or disposal can be found in Appendix A: List of Documents for Retention and Disposal. This is updated regularly in accordance with any changes to legal requirements.

9.2 The management of email/Office 365 accounts for Councillors or employees leaving the Town Council is contained in Appendix B: Management of Councillor and Employee Email/Office 365 Accounts and Mailboxes.

Saltash Town Council

Appendix A: List of Documents for Retention or Disposal

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Minutes	Indefinite	Archive		Original signed paper copies of Town 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)

Document	Minimum Retention Period	Reason	Location Retained	Disposal
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

Document	Minimum Retention Period	Reason	Location Retained	Disposal
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	Location Retained	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

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Town Park equipment inspection reports	21 years			
Investments	Indefinite	Audit, Management		N/A
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management		N/A
Councillors 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	Retained for as long as it is useful and relevant			Bin

Document	Minimum Retention Period	Reason	Location Retained	Disposal
e.g. circulars from county associations, NALC, principal authorities				
Local/historical information	Indefinite – to be securely kept for benefit of the Parish	Town 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

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Magazines and journals	Town Council may wish to keep its own publications For others retain for as long as they are useful and relevant.	The Legal Deposit Libraries Act 2003 (the 2003 Act) requires a local Town Council which after 1st 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		Bin if applicable

Document	Minimum Retention Period	Reason	Location Retained	Disposal
		as defined by the 2003 Act published by a local Town Council therefore constitute materials which the British Library holds.		
	Record-keeping			
To ensure records are easily accessible it is necessary to comply with the following:	The electronic files will be backed up periodically on a portable hard drive and also in the cloud-based	Management		Documentation no longer required will be disposed of, ensuring any confidential documents are

Document	Minimum Retention Period	Reason	Location Retained	Disposal
✓ A list of files stored in cabinets will be kept ✓ Electronic files will be saved using relevant file names	programme supplied by the Town Council's IT company.			destroyed as confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
General correspondence	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	Management		Bin (shred confidential waste) A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
	accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.			
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	After an employment relationship has ended, a Town 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		Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
	Recommend this period be for 3 years	claims made against the Town Council.		
	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

Document	Minimum Retention Period	Reason	Location Retained	Disposal
				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.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Sums recoverable by statute	6 years			Confidential waste.
Personal injury	3 years			Confidential waste.
To recover land	12 years			Confidential waste.
Rent	6 years			Confidential waste.
Breach of trust	None			Confidential waste.
Trust deeds	Indefinite			N/A
For Halls, Centres, Recreation Grounds				
• 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.

Document	Minimum Retention Period	Reason	Location Retained	Disposal
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			

Document	Minimum Retention Period	Reason	Location Retained	Disposal
• 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	Location Retained	Disposal
	Planning Papers			
Applications	1 year	Management		Bin
Appeals	1 year unless significant development	Management		Bin
Trees	1 year	Management		Bin
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
	CCTV			
Daily notes	Daily	Data protection		Confidential waste
Radio rotas	1 week	Management		Confidential waste

Document	Minimum Retention Period	Reason	Location Retained	Disposal
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

Appendix B –Data Retention and Disposal Policy – Management of Councillor and Employee Email/Office 365 Accounts and Mailboxes

This procedure is to be followed when a Councillor resigns from the Town Council or a member of staff leaves the employment of the Town Council.

Councillors:

Town Clerk notified of the resignation.

Town Clerk or delegated Officer - instruct IT Consultant by email to remove access to account immediately.

IT Consultant to archive mailbox and account contents for 12 months.

IT Consultant deletes account, mailbox and all contents after 12 months and notifies Town Clerk or delegated Officer in writing.

Employees:

1. Personal accounts

   Town Clerk or delegated Officer – instruct IT Consultant by email to remove Office 365 access at 5.00pm on last day of employment

   Mailbox to have out of office divert message for three months (keeping the account live)

   After 3 months IT Consultant to archive mailbox for 2 years

   After 2 years – IT Consultant to check with Town Clerk/delegated Officer for email confirmation that the account mailbox can be deleted.

2. Officer role specific accounts (e.g. Town Clerk, Finance Officer, Accounts, HR, Enquiries)

   Town Clerk/delegated Officer – instruct IT Consultant by email to change password at 5.00pm on last day of employment maintaining access for other authorized staff.

3. Accounts where more than one employee has access

Town Clerk/delegated Officer to instruct IT Consultant by email to change password at 5.00pm on last day of employment of departing team member maintaining access for other authorised staff.

4. Teams

Once the IT Consultant has removed Office 365 access is automatically removed. Chats should be deleted from Teams.

Information & Data Protection Policy

Introduction

In order to conduct its business, services and duties, Saltash Town Council processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

Saltash Town Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

This Policy will be linked to our Quality Policy and ICT Policy (to be established) which will ensure information considerations are central to the ethos of the organisation.

The Town Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

The Town Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the

case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is routinely available is contained in the Town Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information

Saltash Town Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulation (GDPR)[1] which became law on 25th May 2018 and will like the Data Protection Act 1998 before them, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Town Council with legitimate reasons for using personal information.

The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

[1] UK GDPR from 01.01.2021

Data Protection Terminology

Data subject - means the person whose personal data is being processed. That may be an employee, prospective employee, associate or prospective associate of STC or someone transacting with it in some way, or an employee, Councillor or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.
It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Town Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
• organizing, adapting or altering it
• retrieving, consulting or using the information or data

• disclosing the information or data by transmission, dissemination or otherwise making it available
• aligning, combining, blocking, erasing or destroying the information or data. regardless of the technology used.

Saltash Town Council processes personal data in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law;
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law;
- monitor its activities including the equality and diversity of its activities;
- fulfil its duties in operating the business premises including security;
- assist regulatory and law enforcement agencies;
- process information including the recording and updating details about its Councillors, employees, partners and volunteers;
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint;
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Town Council;
- undertake research, audit and quality improvement work to fulfil its objects and purposes;
- carry out Town Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Town Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any **sensitive personal information** and the Town Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?

The Town Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Town Council has delegated this responsibility day to day to the Data & FOI Officer.

- Email: gdpr@saltash.gov.uk
- Phone: 01752 844846
- Correspondence: The Town Clerk, The Guildhall, 12 Lower Fore Street, Saltash PL12 6JX

The Town Council may also appoint an external Data Protection Officer to ensure compliance with Data Protection legislation.

Diversity Monitoring & Personnel Data

Saltash Town Council does not monitor the diversity of its employees or Councillors.

The Town Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Saltash Town Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however where ever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Town Council is able to keep their personal data accurate and up-to-date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Councils Right to Process Information

UK General Data Protection Regulations (and Data Protection Act) 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.
Processing is necessary for the legitimate interests of the Council.

Information Security

The Town Council cares 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.
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.

Children

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

Rights of a Data Subject:

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting the Data & FOI Officer.

Information Correction: If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate. Please contact: the Data & FOI Officer.

Information Deletion: If the individual wishes the Town Council to delete the information about them, they can do so by contacting the Data & FOI Officer.

Right to Object: If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Data & FOI Officer.

The Town Council does not use automated decision making or profiling of individual personal data.

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Data & FOI Officer, Data Protection Officer (when appointed) or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

The Town Council will always give guidance on personnel data to employees through the Employee handbook.

The Town Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

The Publication Scheme is a means by which the Town Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Town Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It will be supplemented with an Information Guide which will give greater detail of what the Town Council will make available and hopefully make it easier for people to access it.

All formal meetings of Town Council and its committees are subject to statutory notice being given on notice boards, the website and sent to the local media. The Town Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Town Council welcomes public participation and has a public participation session on each Town Council and committee meeting. Details can be seen in the Town Council's Standing Orders, which are available on its website or at its Offices.

Occasionally, the Town Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Town Council, but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Town Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Town Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Town Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure Information

The Town Council will as necessary undertake checks on both staff and Councillors with the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures

and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Data Transparency

The Town Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

“Public data” means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Town Council’s decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:

Demand led: new technologies and publication of data should support transparency and accountability

Open: the provision of public data will be integral to the Town Council’s engagement with residents so that it drives accountability to them.

Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Saltash Town Council exceeds this turnover but will nevertheless ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports

- List of Councillor responsibilities
- Details of public land and building assets
- Draft minutes of Town Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

Management of Transferable Data Policy

1 Purpose

1.1 This policy supports the controlled storage and transfer of information by Town Councillors and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Town Council) who have access to and use of computing equipment that is owned or leased by Saltash Town Council.

1.2 Information is used throughout the Town Council and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of the Town Council and may result in financial loss and an inability to provide services to the public.

1.3 It is therefore essential for the continued operation of the Town Council that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Town Council's needs.

1.4 The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:

1.4.1 Enabling the correct data to be made available where it is required;
1.4.2 Maintaining the integrity of the data;
1.4.3 Preventing unintended consequences to the stability of the computer network;
1.4.4 Building confidence and trust in data that is being shared between systems;
1.4.5 Maintaining high standards of care towards data and information about individual parishioners, staff or information that is exempt from disclosure;

1.4.6 Compliance with legislation, policies or good practice requirements.

2 Principles

2.1 This policy sets out the principles that will be adopted by the Town Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.

2.2 Removable media includes but is not limited to:
USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems, or stores electronic data separately from email or other applications.

2.4 Any person who intends to store Town Council data on removable media must abide by this Policy. This requirement devolves to Town Councillors, employees and agents of the Town Council, who may be held personally liable for any breach of the requirements of this policy.

2.5 Failure to comply with this policy could result in disciplinary action.

3 Advice and Assistance

3.1 The Town Clerk will ensure that everyone that is authorised to access the Town Councils information systems is aware of their obligations arising from this policy.

3.2 A competent person should be consulted over any hardware or system issues. Advice and guidance on using software packages should be also sought from a competent person.

4 Responsibilities

4.1 The Town Clerk is responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Town Council business.

4.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

5 Incident Management

5.1 It is the duty of all employees and agents of the Town Council to not allow storage media to be compromised in any way whilst in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to the Town Clerk.

5.2 It is the duty of all Town Councillors/Employees to report any actual or suspected breaches in information security to the Town Clerk.

6 Data Administration

6.1 Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.

6.2 Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.

6.3 Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.

6.4 Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken so as to easily identify the version of the data, as well as its content.

6.5 Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. The Town Council's retention and disposition schedule must be implemented by Town Councillors, employees, contractors and agents for all removable media.

7 Security

7.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

7.2 Virus Infections must be prevented from damaging the Town Councils network and computers. Virus and malware checking software approved by the Town Council, must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.

7.3 Any memory stick used in connection with Town Council equipment or to store Town Council material should usually be Town Council owned. However work related data from external sources can be transferred to the Town Council network using memory sticks that are from trusted sources and have been checked using current anti-virus software.

7.4 The Town Council will not provide support or administrator access for any non-Town Council memory stick.

8. Use of removable media

8.1 Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.

8.2 Town Council material belongs to the Town Council and any equipment on which it is held should be under the control of the Town Council and not available to be used for other purposes that may compromise the data.

8.3 All data transferred to removable media should be in accordance with an agreed process established by the Town Council so that material can be traced.

8.4 The person arranging the transfer of data must be authorised to make use of, or process that particular data.

8.5 Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.

8.6 Encryption must be applied to the data file unless there is no risk to the Town Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available then password control must be applied if removable media must be used for the business purpose.

9 Faulty or Unneeded Storage Devices

9.1 Damaged or faulty media must not be used. The Town Clerk must be consulted over any damaged equipment, peripherals or media.

9.2 All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device.

10 Breach procedures

10.1 Users who do not adhere to this policy will be dealt with through the Town Councils disciplinary process.

10.2 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

11 Review and Revision

11.1 This policy will be reviewed annually by the Town Council and revised according to developments in legislation, guidance, accepted good practice and operational use.

12 Employees Guide in Brief

12.1 Data and information are valuable and must be protected.

12.2 Only transfer data onto removable media, if you have the authority to do so.

12.3 All transfer arrangements carry a risk to the data.

12.4 Run the virus checking programme on the removable media each time it is connected to a computer.

12.5 Only use approved products for Town Council data.

12.6 Activate encryption on removable media wherever it is available and password protection if not available

12.7 Data should be available for automatic back up and not solely saved to removable media.

12.8 Delete files from removable media, or destroy the media, after the material has been used for its purpose.