



## APPENDIX B

# SALTASH TOWN COUNCIL

---

GDPR INSPECTION REPORT SEPTEMBER 2025

Paul Russell

PATAS | 2 SCHOOL VILLAS, CROSSLANDS, TONEDALE, WELLINGTON SOMERSET TA21 0AF

---

# **CONTENTS**

<b>1.</b>	<b>Introduction.....</b>	<b>2</b>
<b>2.</b>	<b>Identification of Personal Data Held.....</b>	<b>2</b>
<b>3.</b>	<b>Collection of Personal Data.....</b>	<b>3</b>
<b>4.</b>	<b>Record Management.....</b>	<b>7</b>
<b>5.</b>	<b>Information Sharing.....</b>	<b>8</b>
<b>6.</b>	<b>Conclusion.....</b>	<b>8</b>

## **1. INTRODUCTION**

- 1.1 The Data Protection Act 2018 required organisation that collected personal data, including local authorities, to implement a range of requirements to carry out their services.
- 1.2 The Act has recently been updated through both the UK GDPR Regulations and The Data (Use and Access) Act 2025 (DUAA) which was passed into law on 19<sup>th</sup> June 2025.
- 1.3 The Key changes being made under the DUAA that affect local authorities are as follows:
  - Data Subject Access Requests: Searches only need to be reasonable and proportionate, and response deadlines altered. If information is withheld exemption must be explained.
  - New Right to Complain: Complainants can complain directly to the organization about how their data is being used. 30 calendar days allowed to respond. New privacy policy and complaints procedure required.
  - Introduction of certain “Recognised Legitimate Interests”: No longer necessary to balance rights and freedoms of individuals. Focused mainly on safeguarding of vulnerable individuals.
  - Disclosures to other organisations: Organisations requesting information relating to Public Task (e.g. The Police) now responsible for providing the reason rather than the information provider.
  - Special Category Data: Additional categories may be added by Secretary of State but existing ones remain unchanged.
  - Reusing personal information: Information can be reused by second data controller in certain circumstances (archiving for the public interest and safeguarding). Focuses on data shared between organisations.
  - ICO to be replaced by IC. Different structure and new investigative powers
  - Changes will come into force within the next 12 months.
- 1.4 The DUAA amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).
- 1.5 The audit is in 4 parts and each of the four parts have been reviewed as part of this audit:
  - Identification of what personal data is held
  - Collection of personal data
  - Records management
  - Information sharing

## **2. IDENTIFICATION OF PERSONAL DATA HELD**

- 2.1 In order to carry out its functions and deliver its services Saltash Town Council does collect personal data.
  - 2.2 The following areas collect personal data within the Town Council:
-

- Finance & Administration;
- Councillor information;
- HR, Payroll, Personnel;
- Cemetery Services;
- Allotment Services;
- Civic Functions;
- Facility Hirers;
- Venues and facilities for hire;
- Newsletter;
- Website and Social Media;
- Complaints/enquiries;
- Markets.

2.3 All data storage for Saltash Town Council is located at The Guildhall, Lower Fore Street, Saltash, PL12 6JX. Some additional data is also held at the Council's depot at Longstone Garage and Store, Glebe Avenue, PL12 6DN.

2.4 The Town Council keeps both electronic and paper based records but is working towards a paperless environment. Electronic data is managed by the Council's IT company and there are the appropriate security measures in place. **It is recommended that confirmation of the Council's IT provision is confirmed with the IT company including how often data is backed up during each day and whether monthly backups are taken and kept offsite in a secure location.**

Privacy notices are currently not included on relevant documentation such as booking forms, grant application forms etc. A basic short privacy notice has been provided and this should be included on all forms.

There is a Council Privacy Notice on the website which is available for download and provides information on how data is used by the Council.

A Data Protection Policy and a Data Retention Policy has been adopted and was updated in 2024. Due to the passing into law of the Data (Use & Access) Act 2025 this will need to be reviewed again within the next 12 months.

The Data Retention Policy includes the deletion, erasure and updating/correcting of information.

The Data Breach Policy and Subject Access Request Policy are in place. The SAR Policy can be downloaded but the Data Breach Policy is not available. This needs to be addressed.

All staff are aware of GDPR and it has now become part of the Council culture to consider Data Protection as part of carrying out daily tasks. Regular reminders are sent out and training is provided.

2.5 Biometric data includes technology that identifies employees based on physical characteristics, such as fingerprints, iris colour, or voice recognition.

The most common use of biometric data at present is fingerprints (smartphone access) and voice recognition. The Town Council does not actively collect any biometric information but mobile devices do record this information. In the event of a change of personnel the information is deleted and the mobile device is set back to standard factory settings.

- 2.6 Personal information is updated when up to date personal data is received. The Town Council is aware that personal data needs to be updated regularly and is constantly reviewing its procedures to ensure that data retained is as accurate as possible. Each department deals with the updating of personal information based on the way it delivers the service and departmental processes are reviewed.

A process to update Cemetery records regularly to ensure contacts are correct needs to be developed.

Allotment records are updated annually.

Civic lists are updated annually and consent sought where required.

Pontoon information is updated on an ad-hoc basis.

Event information is updated as required.

Booking of venues contact information is retained according to the Retention Policy and updated on an ad-hoc basis.

Email lists are managed by the Officer in charge. The Council does not hold many mailing lists except for Civic functions and some events. These are updated as required.

The majority of data collection is undertaken electronically and there are processes in place to update and delete information in line with GDPR requirements.

### 3. COLLECTION OF PERSONAL DATA

3.1 The Town Council collects personal data as identified below

<b>Class of Record</b>	<b>Purpose</b>
Personnel Records	<ul style="list-style-type: none"> <li>• To keep a record of all staff employed by the Town Council;</li> <li>• Contract requirement;</li> <li>• Health &amp; Safety;</li> <li>• Insurance;</li> <li>• Legal requirement.</li> </ul>
Councillor personal information	<ul style="list-style-type: none"> <li>• To deliver democratic representation to the local community;</li> <li>• To provide open and transparent governance;</li> <li>• Health &amp; Safety;</li> <li>• Insurance</li> </ul>
Contractor information	<ul style="list-style-type: none"> <li>• To keep a record of all contractors providing services for and on behalf of the Town Council;</li> <li>• To pay outstanding accounts;</li> <li>• Contract requirement;</li> <li>• Health &amp; Safety;</li> <li>• Insurance;</li> <li>• Legal requirement.</li> </ul>
Residents	<ul style="list-style-type: none"> <li>• Service delivery;</li> <li>• Improving, developing and addressing service issues;</li> <li>• Electoral role;</li> <li>• Improving the Town Council.</li> </ul>
Businesses	<ul style="list-style-type: none"> <li>• Service delivery;</li> <li>• Improving and investing in the Town</li> </ul>
Hirers	<ul style="list-style-type: none"> <li>• Service delivery;</li> <li>• Contract requirement</li> <li>• Health &amp; Safety;</li> <li>• Insurance;</li> <li>• Legal requirement.</li> </ul>
Complaints	<ul style="list-style-type: none"> <li>• Service delivery;</li> <li>• Improving, developing and addressing service issues;</li> <li>• Improving the Town Council.</li> </ul>
Volunteers	<ul style="list-style-type: none"> <li>• To keep a record of all volunteers providing voluntary services to enable a range of services to be delivered;</li> </ul>

	<ul style="list-style-type: none"> <li>• Contract requirement;</li> <li>• Health &amp; Safety;</li> <li>• Insurance;</li> <li>• Legal requirement.</li> </ul>
Cemetery	<ul style="list-style-type: none"> <li>• Legal requirement to maintain burial records;</li> <li>• Contract requirement with regard to leasing plots;</li> <li>• Service delivery;</li> <li>• Health &amp; Safety;</li> <li>• Insurance.</li> </ul>
Allotments	<ul style="list-style-type: none"> <li>• Legal requirement to maintain allotment register;</li> <li>• Contract requirement with regard to leasing plots;</li> <li>• Service delivery;</li> <li>• Health &amp; Safety;</li> <li>• Insurance.</li> </ul>
Events	<ul style="list-style-type: none"> <li>• Risk Assessment;</li> <li>• Health &amp; Safety;</li> <li>• Insurance;</li> <li>• Legal requirement.</li> </ul>

3.2 The Town Council includes one or more of the lawful basis for collecting information in its privacy notices. These are outlined below:

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Note that the Data (Use & Access) Act 2025 may have an effect on the above lawful basis reasons

3.3 The legal basis for collecting the personal information has not altered and is as follows:

<b>Class of Record</b>	<b>Legal Basis</b>
Personnel Records	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation;</li> <li>• Vital Interests.</li> </ul>
Councillor personal information	<ul style="list-style-type: none"> <li>• Explicit Consent;</li> <li>• Public Interest;</li> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation.</li> </ul>
Contractor information	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation.</li> </ul>
Residents	<ul style="list-style-type: none"> <li>• Public Interest;</li> <li>• Compliance with legal obligation;</li> <li>• Explicit Consent.</li> </ul>
Businesses	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation;</li> </ul>
Hirers	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation;</li> <li>• Explicit Consent.</li> </ul>
Complaints	<ul style="list-style-type: none"> <li>• Public Interest;</li> <li>• Compliance with legal obligation;</li> <li>• Explicit Consent.</li> </ul>
Cemetery	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation.</li> </ul>
Allotments	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation;</li> <li>• Explicit consent.</li> </ul>
Events	<ul style="list-style-type: none"> <li>• Contractual necessity;</li> <li>• Compliance with legal obligation;</li> <li>• Explicit Consent.</li> </ul>

All Privacy Notices contain the legal basis outlining the reason why the Town Council is collecting the information.

Privacy notices are in place for data collection requirements but they do need to be updated in some areas.

An email response privacy notice is included on all emails outlining the Town Council's commitment to Data Protection.

The website includes data protection information, the rights of the individual to access their information and contact information of the ICO.

3.4 Consent, where required, is normally sought and obtained verbally. Consent is recorded where necessary. General enquiries are managed under the Data Protection Act 2018 requirements.

#### **4. RECORD MANAGEMENT**

4.1 Records are stored at the Town Council Offices. A range and variety of records are stored, some of which contain sensitive personal information. Council has a Cloud based IT infrastructure in place.

4.2 Storage of electronic files are held on the Cloud and back-up is carried out offsite. This is managed by the Council's IT consultant. Ensure that all files are securely protected and backed up on a daily basis by the IT company to help reduce any data lost through possible ransom attacks and other virus attacks.

4.3 Access to records are based on the sensitivity of the records being stored. The Council has two restricted drives and a shared drive. It is good practice to protect some sensitive files with passwords to help protect very sensitive information.

4.4 The following electronic access controls are in place:

- Password protected computer access;
- Restricted physical access to the Council Offices;
- Payroll is on a restricted drive which has password protection in place;
- All computers and software access are password protected;
- Sensitive files and folders have restricted access.

All computers have antivirus protection;  
The IT infrastructure is being transferred to a new Cloud based system provided by a Sector acknowledged service provider;  
Ensure that there continues to be restricted access drives for sensitive information and services

4.5 The following manual access controls are in place:

- The main Council Offices are locked and alarmed when not in use;
- Restricted access to the Offices and storage areas;
- The building has an alarm fitted;
- All offices can be locked when not in use.

4.6 The following manual storage systems are in place:

- Secured filing cabinets;
- Secured filing cabinets;
- Secured desk drawers;
- Secured cupboards.

4.7 Data retention processes are now being implemented.

- The Data Retention policy has been adopted but needs to be reviewed;
- Records no longer required are disposal of and electronic records are erased as required;
- Personal information is updated on a regular basis depending on the service being delivered;
- Service Level Agreements are GDPR compliant;
- All computers are running on Windows 11. Note that support for Windows 10 comes to an end in October 2025.

4.8 Town Council emails are stored on the Cloud in the UK. All staff and Councillor emails are xxx@saltash.gov.uk.

4.9 Assertion 10 of the Practitioners Guide requires Councils to have their own domain name for emails as well as some other requirements.

4.9 The Council uses the Outlook email client for its emails. Each staff member manages their emails differently but they all delete emails that are no longer required and only store emails that are essential for the delivery of Council services.

## **5. INFORMATION SHARING**

5.1 The Town Council shares some of its information with various contractors and agencies to enable it to deliver its services and operate efficiently. The sharing of data is outlined in its Data Protection policy and the relevant privacy notices.

5.2 There are data sharing agreements in place for the sharing of personal data with Council agents, suppliers and contractors as well as other data controllers, such as local authorities, community groups, charities and credit reference agencies.

## **6. CONCLUSION**

6.1 The Town Council proactively reviews its responsibilities under the Data Protection Act 2018 and undertakes regular Data Audit Reviews.

6.2 It also contracts an external DPO and Data Protection Advisor to help it meet all its data protection obligations.

6.2 An Action Plan has been provided. The Town Council continues to keep Data Protection under review and has put in place systems to assess compliance in the future, such as a Data Protection Officer, recommended as best practice, and Data Privacy Impact Assessments (DPIA) for new projects.

6.4 The following actions need to be considered:

- The website needs to be updated with the relevant Data Protection Policies;
- All Councillors need to have completed their consent form regarding personal information being publicised;
- A new IT policy under Assertion 10 of the Practitioners Guide needs to be drafted and adopted;
- The Data Protection Policy will need to be reviewed and updated within the next 12 months to ensure it meets the requirements of the DPA 2018 and the DUAA 2025;
- The Data Audit review will need to be considered by the relevant Committee;
- Continue to include privacy notices on all relevant documentation. Ensure that the website privacy notice is reviewed and updated;
- Note that any new service delivery will require a Data Protection Impact Assessment to be carried out.