Somerton Town Council

working with the community

Somerton Town Council
Policy Documents
Data Protection Policy

Adopted: 12th April 2016
Re-Adopted: January 2020
Review Date: February 2024

DATA PROTECTION POLICY

1 Introduction

1.1 Somerton Town Council needs to collect and use certain types of information about people with whom it deals in order to operate. This includes information relating to current, past and previous employees, suppliers, customers and others with whom it communicates.

1.2 Somerton Town Council is registered with the Information Commissioner's Office under Register reference: Z2595957

1.3 There is a clear distinction between 'personal' data and 'sensitive personal' data.

- 'Personal' data is data defined as relating to a living individual who can be identified from:
  a) that data; or
  b) that data plus other information which is in the possession of the Data Controller and includes an expression of opinion about the individual.

- 'Sensitive Personal' data is defined as personal data consisting of information relating to:
  a) Racial or ethnic origin;
  b) Political opinion;
  c) Religious or other beliefs;
  d) Trade union membership;
  e) Physical or mental health or condition;
  f) Sexual orientation; or
  g) Criminal proceedings or convictions.

1.4 In accordance with the Data Protection Act 2018, all organisations which process personal

information (whether on paper, in a computer, or recorded on any other media) are required to comply with a number of important principles regarding privacy and disclosure.

This ensures that the information is:

- Processed fairly and lawfully;
- Only processed for the purpose it was obtained;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than necessary;
- Processed in line with the data subject's rights;
- Secure; and
- Not transferred to other countries without adequate protection.

1.5 Through appropriate management Somerton Town Council will strictly apply the following criteria and controls:

- Fully observe conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process relevant information, only to the extent that is required to fulfill operational needs/to comply with legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time that information is held;
- Ensure that the rights of the people about whom information is held, are able to be fully exercised under the Act;
- Take appropriate technical and organisational security measures to safeguard personal information; and
- Ensure that personal information is not transferred abroad without suitable safeguards.

1.6 Somerton Town Council will also ensure that:

- There is someone with specific responsibility for Data Protection in the organisation (the person currently nominated is the Town Clerk);
- Everyone managing and handling personal information
    a) fully understands that they are contractually responsible for following good practice in terms of protection;
    b) is adequately trained to do so; and
    c) are appropriately supervised.

2 Rights to Access Information

2.1 Staff, Councillors, residents, customers and other data subjects have the right to:

- Ask what the Council uses the information for;
- To be provided with a copy of the information;
- To be given details of the purposes for which the Council uses the information and any other persons or organisations to whom it is disclosed;

- To ask that any incorrect data held is corrected.

2.2 Any person wishing to see information held about them should write to the Council, addressing the letter to the Town Clerk. Information required includes name and address, proof of identity, date of birth and any other information which would assist in finding their information. The Council will respond within 28 days of receipt of application.

2.3 If an individual notifies the Council that the data is incorrect and requests that it be amended, the Council must advise the individual within 21 days whether or not the amendment has been made.

3 Breach of Policy

3.1 Compliance with the Act is the responsibility of all Councillors, residents, customers and members of staff. Any deliberate or reckless breach of the Policy may lead to disciplinary action and where appropriate, legal proceedings.

3.2 Any individual who believes that the Council has breached any of the requirements of the Data Protection Act 1998 should raise the matter with the Data Controller initially. Alternatively, a complaint can be made to the Information Commissioner's Office via their website at https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/

3.3 Loss of an unencrypted laptop, phone or other device used by a Councillor or employee for work purposes will constitute a breach of data security and must be reported to the Data Controller using the form found at Appendix A.

4 Freedom of Information

In accordance with the Freedom of Information Act 2000, this Document will be posted on the Council's Website http://www.somertontowncouncil.gov.uk/policies-and-procedures/ and copies of this document will be available for inspection on deposit in the Council Office.

5 Review

5.1 This policy will be reviewed every year (or earlier if required by changes to legislation or additional documentation) and amended as necessary based on good practice or evidence taken forward.

APPENDIX A: DATA SECURITY BREACH REPORTING FORM

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is stored, inappropriate access control allowing unauthorised use, equipment failure, human error, unforeseen circumstances such as fire or flood, hacking attack, blagging offences where information is obtained by deceiving the organisation who holds it etc. Examples includes: Reportable theft or loss of an unencrypted laptop or other unencrypted portable electronic/digital media holding names, addresses, dates of birth, or NI numbers of individuals; loss or theft of a manual paper-based filing system holding personal data relating to named individuals and their financial records etc. More information can be found at: https:/ico.org.uk/media/for-organisations/documents/1562/guidance on data security breach management.pdf

This form is to be used to report such breaches or suspicion of the occurrence of a breach.

Breach containment and recovery
Article 2(2) of the Notification Regulation states:
The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex 1. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date and time of notification of breach	
Notification of breach to: Name Contact details	
Details of breach	
Nature and content of data involved	

Number of individuals affected	
Name of person investigating breach Name Job title Contact details	
Information Commissioner informed: Time and method of contact https://report.ico.org.uk/security-breach/	
Police informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many contacted? Method of contact used? Does the breach affect individuals outside the UK? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it and the likely cost to them of taking those measures is relayed to the individuals involved	

Staff briefed	
Assessment of ongoing risk	
Containment actions: technical and organisational security measures applied to the affected personal data	
Recovery plan actions	
Evaluation and response	