Records Management Policy

1. Introduction

Trowbridge Town Council 'The Council' is committed to meeting the principles of the *General Data Protection Regulations (GDPR)* and the *Data Protection Act 2018.*

Article 5(1)(e) requires that:

> *'Personal data shall be kept in a form which permits identification of subjects for no longer than is necessary for which the personal data are processed.'*

This Policy and attached retention schedule should be used as the basis for the management of personal data and more widely all data processed by Trowbridge Town Council. Establishing effective Information Governance systems requires the purpose, legality and period of processing to be identified prior to undertaking the handling of any data. Processing refers to the capture, storage, use, transfer and disposal of data.

2. Scope and Application

All staff, including councillors and volunteers who handle personal data are responsible for ensuring that they are aware of this Policy and, where any concern that personal data is being handled beyond the period for which it should be, they should raise their concern with the Data Protection Officer (DPO).

Officers are responsible for ensuring that any existing system, or new system has, by design, appropriate and effective measures in place for the marking or tracking of personal data from collection to its applicable date of disposal.

This policy applies to all records irrespective of format. Consideration should always be made where the format may increase potential vulnerabilities. The application of the data protection principle of security will always apply (Art.6(1)(f), GDPR).

A record may refer to any piece of information created or received and maintained by an organisation or person in the course of their business or conduct of their affairs and kept as evidence of such activity.

Records must be kept in such a format that they are accurate, accessible, secure, and safely disposed of and appropriate safeguards must always be in place to ensure an adequate level of security is applied commensurate to the sensitivity of the record.

3. Definition of Retention Periods

Defining a retention period will be determined by one of the following three factors:

- Statutory requirements.
- Codes of Practice and guidance published by professional bodies.
- In the absence of the above, the retention period will be determined by the needs of the Council.

Defining the retention period based on Council needs must be approved by the Town Clerk or relevant senior manager and where necessary in consultation with the DPO.

4. Reviewing Retention Periods

Most retention periods will remain static and will relate to legal requirements to retain data. However, retention periods based on law and codes of practice and guidance published by professional bodies may vary. Any changes to known retention periods should be raised with the Town Clerk and where necessary the DPO.

This Policy and retention schedule should be reviewed every four years or where any other cause requires its immediate correction.

5. Course of Action at the End of the Retention Period

When a record reaches the end of its retention period in most cases it will be deleted or destroyed. However, these are not the only courses of action that can be taken, and consideration must be made to the relevance of the data for other uses.

In most cases the requirement for further use of data will be identified prior to processing, however there may be occasion where a dataset is identified as having particular relevance to the needs of the Council.

The following may occur to data after the period of use has expired:

- Anonymisation for statistical needs.
- Transfer to an appropriate archive where it is a legal requirement or in the public interest.
- Scientific or historical research purposes.
- Appropriate safeguards must be put in place to ensure that wherever personal data is used beyond its original period of retention it is done so legally and in compliance with the Data Protection Act 2018 and guidance from the Information Commissioners Office (ICO).

6. Record Disposal

Systems such as Outlook will generally have in-built settings that automatically delete records once they have reached the end of their retention period. However, it is necessary to ensure that the system is effectively managed and flagged records are reviewed and deleted. Where a system may automatically delete records adequate measures such as data quality assessments must be taken to ensure that this has occurred correctly. When using personal data outside of an automatic deletion a structure of storage must be created to allow for the proper control of personal data. This may be in such a way as labelling electronic or physical folders with expiry dates or using a hierarchy that indicates the date of creation. Physical records must be disposed of in a manner corresponding to their sensitivity. If records containing Special Category (SC) personal data are to be destroyed, they must be securely shredded. Where applicable a record of destruction should be maintained. This should include the type of data or, grouping of data, the period it correlates to and, date of destruction and an authorising signature.

7. Protective Marking

Protective markings may be written upon documentation where it is used in physical forms. In general, the classification of documentation will relate more specifically to the handling and access that is permitted to that data. Confidential data related to employment purposes for example should only be accessible by HR staff or direct line managers for specific reasons.

Information deemed to be financially sensitive, or business sensitive may for the purposes of requests made under the Freedom of Information Act be exempt and, in any case, should be handled with more caution than general data.

Review this policy on 07/07/2024
On change of DPO or Clerk
On any significant change to adopted procedures

Retention Schedule
Our schedule sets out

What is the purpose of the information we collect?
Who is responsible for this data (information custodian)?
How long do we keep a type of data for, and what countdown process must we follow?
Whether the retention period is defined by law or based on common business practice.

We must:

Identify records we need to keep and dispose of records we no longer legally need or process.
Define how long information is kept.
Confirm how information is stored at different stages of the process.
Provide evidence that records are/have been disposed of.

Policy approved on 7/7/2020

Signature……Dated…….