SOUTH STAFFORDSHIRE DISTRICT COUNCIL DATA RETENTION POLICY

1. Introduction

1.1 The Council gathers information, records and data from both individual members of the public and external organisations. Data is important to how the Council carries out its functions and duties, meets its operational needs and manages its employees and in order to have information available when it is needed.

1.2 There are legal and regulatory requirements for the Council to retain certain data, usually for a specified amount of time. However, it does not need to retain all data indefinitely, and retaining data can expose the Council to risk and costs.

1.3 This Data Retention Policy explains the requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.4 Failure to comply with this policy can expose the Council to fines and penalties, adverse publicity, difficulties in providing evidence when it is needed and meeting the operational needs of the Council.

1.5 Compliance with this policy is mandatory and any breach may result in disciplinary action. It may be amended at any time.

2. Error! Bookmark not defined.SCOPE OF POLICY

2.1 This policy covers all data that the Council holds or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy this information and these records are collectively referred to as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage.

2.3 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data.

3. GUIDING PRINCIPLES

3.1 Through this policy, and data retention practices, the Council aims to meet the following commitments:

- To comply with legal and regulatory requirements to retain data.
- To comply with data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- To handle, store and dispose of data responsibly and securely.
- To create and retain data where this is needed to operate effectively, but not to create or retain data without good business reason.
- To allocate appropriate resources, roles and responsibilities to data retention.

- To regularly remind employees of their data retention responsibilities.

- To regularly monitor and audit compliance with this policy and update this policy when required.]

4. Error! Bookmark not defined.**ROLES AND RESPONSIBILITIES**

4.1 **Responsibility of all employees** to aim to comply with the laws, rules, and regulations that govern the Council and with recognised compliance good practices. All employees must comply with this policy, the Record Retention Schedule, any communications suspending data disposal and any specific instructions from the Data Protection Officer. Failure to do so may subject the Council and its employees, and contractors to serious civil and/or criminal liability. It is therefore the responsibility of everyone to understand and comply with this policy.

4.2 **Data Protection Officer.** The Council's Data Protection Officer (DPO) is responsible for advising on and monitoring compliance with data protection laws which regulate personal data.

5. TYPES OF DATA AND ITS RETENTION

5.1 **Formal or official records.** Certain data is more important and is therefore listed in the Record Retention Schedule with a specified retention period. This may be because there is a legal requirement to retain it, or because it may be need as evidence of the Council's financial transactions, or because it is important to the operation of the Council.

5.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the relevant service manager once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record. The Record Retention Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed. Examples may include:

- Duplicates of originals that have not been marked or amended.

- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.

- Books, periodicals, manuals, training binders, and other printed materials obtained from external sources and retained primarily for reference purposes.

- Spam and junk mail.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals or information relating to a living individual that can identify (directly or indirectly) from that data alone or in combination with other identifiers. This includes special categories of personal data such as health data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Data protection laws require personal data to be retained for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, account has been taken of the principle of storage limitation balanced against the requirements to retain the data.

5.4 **Confidential information belonging to others**. Any confidential information that may have been obtained from a source outside of the Council, must not, so long as such information remains confidential, be disclosed or used. Unsolicited confidential information submitted should be refused, returned to the sender where possible, and deleted, if received via the internet.

5.5 **What to do if data is not listed in the Record Retention Schedule.** If data is not listed in the Record Retention Schedule, it may be that it should be classed as disposable information. In the first instance guidance should be sought from the service manager with the relevant operational knowledge.

6. STORAGE, BACK-UP AND DISPOSAL OF DATA

6.1 **Storage.** Data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to the Council's operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site in accordance with the Business Continuity Plan.

6.2 **Destruction**. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with Digital Services.

6.3 The destruction of data must stop immediately upon notification from the Data Protection Officer, the Legal Services Team **or** Finance Team that preservation of documents for contemplated litigation, or compliance with government investigation or audit is required (sometimes referred to as a litigation hold).

7. WHERE TO GO FOR ADVICE AND QUESTIONS

7.1 **Questions about the policy.** Any questions about retention periods should be raised with your service manager/team manager. Any questions about this policy should be referred to the Data Protection Officer, Lorraine Fowkes, who is in charge of administering, enforcing, and updating this policy.

8. OTHER RELEVANT POLICIES

8.1 This policy supplements and should be read in conjunction with other policies and procedures in force from time to time, including without limitation the:

- Data Protection Policy
- ICT security and acceptable use policy
- Ways of Working Policy
- Business continuity policy
- And any other IT, security and data related policies, which are available on the intranet

REVIEW DATE (by) 1 November 2024

ANNEX A RECORD RETENTION SCHEDULE