Bromsgrove District and Redditch Borough Councils

Data Standards Policy

Purpose People Pride Performance

Date issued: Jan 2025

Version number: 1

Bromsgrove District Council
www.bromsgrove.gov.uk

Redditch Borough Council
Working together for our communities

Contents

1. Introduction

Effective management and utilisation of data is increasingly important in our digitally connected council. As the Local Authority we are custodians of our resident's data and information, we must ensure that data is collected, stored, shared and disposed of in a standardised, compliant, and secure manner.

This Data Standards Policy is designed to serve as a guide to ensure consistent practices and procedures are implemented for data management by outlining the standards, guidelines, and responsibilities that we must adhere to in all transactions and interactions with data whilst emphasising the importance of protecting sensitive information and complying with data protection regulations.

By establishing clear standards, this policy aims to enhance data quality, accessibility, and interoperability across all service areas, systems, and external stakeholders.

Maintaining the ongoing integrity and quality of data is vital to enable effective decision-making and improved service delivery for our customers.

This policy applies to all council employees, contractors, and third-party service providers who handle council data, including, but not limited to digital files, databases, paper records, and information systems. It includes data collected, processed, and shared within council operations, and data exchanged with external partners, government agencies, and members of the public.

Senior Leadership Team and Corporate Leadership Team supported by the System and Data Governance Board and Group (made up of ICT, Business and Data Improvement Officers and other enabling Service Managers) will ensure that appropriate resources and training are provided to support implementation and compliance with this policy.

A Summary Policy Document providing an overview of the key aspects of this policy is shown in Appendix Three.

2. Data Governance and Documentation

Data governance and documentation are vital in today's connected data-driven world. Effective data governance helps the organisation to maximise the value of its data, mitigate risks, and comply with regulatory requirements.

Documentation involves the systematic recording of data-related strategies, policies, processes, guidelines, standards and procedures. It provides a comprehensive reference point for data governance practices, ensuring transparency, clarity, and consistency in data management.

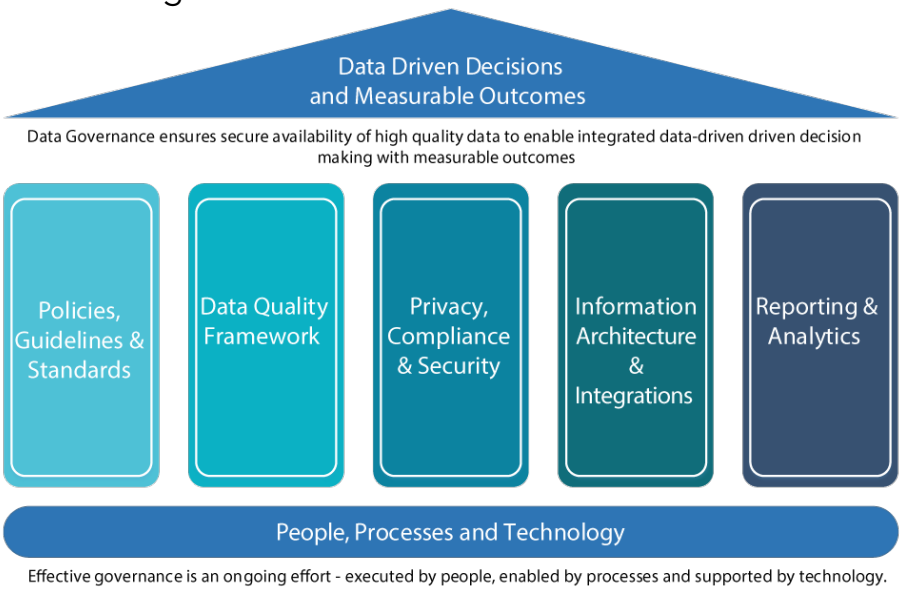


Image source: https://cio.ubc.ca/node/3215

Data Governance:

A System and Data Governance Board has been established to provide governance for the overall management, control, and protection of the organisation's data assets. The Board will be responsible for establishing strategies, policies, processes, standards and guidelines to ensure the proper collection, storage, usage, and sharing of data.

The Systems and Data Governance Board aims to promote data quality, consistency, integrity, and security across the organisation.

Key components of data governance include:

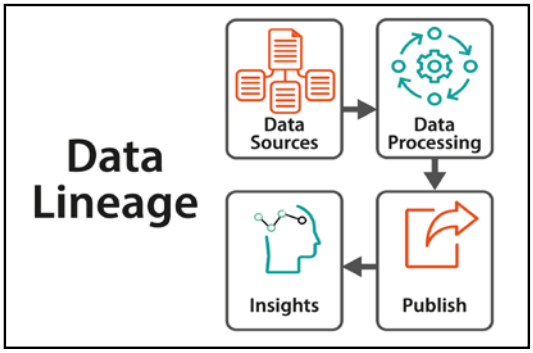
- **Data, Performance, and Insight Strategy:** a strategic plan that aligns data management practices with business objectives, defining data governance goals, and establishing roles and responsibilities.
- **Data Policies and Strategies:** strategies, policies, guidelines and standards that dictate how data should be managed, including data quality standards, data retention policies, and data access and usage guidelines.
- **Data Business Management:** designating people in service areas (Data Stewards) who are responsible for ensuring data integrity, compliance with policies, and promoting data quality within their respective services.
- **Data Lifecycle Management:** managing data throughout its lifecycle, including data collection, storage, retention, sharing, and disposal, in compliance with our data protection and retention practices and the customers rights.
- **Data Quality Management:** implementing processes and controls to monitor and improve the quality of data, including data validation and cleansing against an agreed data model.

Documentation:

By documenting data governance practices, the organisation can establish clear guidelines, facilitate communication, ensure consistency, ownership and provide a reference for training and auditing purposes. It helps in promoting transparency, accountability, collaboration, knowledge sharing and compliance with regulations and industry best practices. It can also enhance decision-making by supporting more reliable and actionable insights from data assets by having a structured and comprehensive record of data-related processes, policies and procedures.

Effective documentation includes:

- **Data Dictionary:** a document that defines and describes the data elements, their attributes, and relationships for each system. It helps in standardising terminology and promoting consistent understanding of data across the organisation. This should be developed when new systems are implemented.



- **Data Lineage Diagrams:** visual representations of how data moves within a system and in the wider organisation, illustrating data sources, transformations, and destinations. Data flow diagrams help in understanding data dependencies and identifying potential risks or bottlenecks.
- **Data Strategies, Policies, Procedures and Information Asset Register:** documenting the strategies, policies, standards and guidelines, and procedures related to data and information management, data security, data privacy, and data usage. These documents provide a reference for employees to understand and adhere to data governance principles.
- **Responsibilities:** clear responsibilities for data input to ensure staff understand what is required of them in their roles.
- **Data input standards, processes, and guidelines:** to provide staff with a reference point for accurate and consistent data entry (Appendix One)

3. Data Principles

The System and Data Governance Board will be the platform for decisions relating to the key data principles below:

- **Data Quality, Validation and Verification:** Data shall be accurate, complete, relevant, and timely, with defined procedures for data validation, verification, and cleansing. KPIs will be used to measure performance2.
- **Standardised Data Formats:** These should be used to provide a common structure and syntax to allow data to be easily shared, exchanged, and interpreted across different systems, applications, and organisations. Standardised data formats facilitate interoperability and promote seamless data integration and analysis.
- **Data Sharing and Interoperability:** Council departments shall adopt common data formats, standards, and protocols to facilitate seamless data sharing and interoperability between systems and external stakeholders.
- **Data Retention and Disposal:** Retention periods for distinct types of data shall be defined, along with secure disposal methods to ensure compliance with data protection legislation.
- **Data Access and Transparency:** Council data shall be made accessible to the public in accordance with Freedom of Information and Transparency requirements, while safeguarding sensitive or confidential information. (see section 9).
- **Data Privacy and Security:** Measures shall be implemented to protect data from unauthorised access, loss, alteration, or disclosure, in compliance with data protection laws and regulations. Personal and sensitive information shall be managed in accordance with data protection principles, respecting individuals' rights to privacy and confidentiality. The Council is committed to maintaining the following relevant accreditations to ensure that we meet the minimum standards imposed by legislation and regulation: Public Services Network (PSN), Data Security and Protection (DSP) Toolkit, NHS Data Security and Protection Toolkit.

4. Data Quality, Validation and Verification

The System and Data Governance Board will be the platform for decisions relating to the data quality, validation, and verification, including identifying measurable KPIs:

Data validation and verification are critical for maintaining high-quality data. They are essential processes in data management that ensure the accuracy, completeness, and reliability of data. They help prevent errors, identify discrepancies, and improve the trustworthiness of data for effective decision-making, reporting, and operational processes. Both processes are typically performed before data is entered into a system or used for analysis and decision-making.

Data Validation

Data validation involves checking the integrity and quality of data to ensure it meets predefined rules, standards, and requirements. It provides an opportunity to verify whether the data to be used in the system is valid, consistent, and appropriate for its intended use.

The main objectives of data validation are:

- **Completeness:** Ensure that all required fields or data elements are present and populated accurately.
  - **KPI examples:** % missing values, % fields that contain data, Ratio of complete records to total number of records.
- **Accuracy:** Verify that data is entered correctly and matches the expected values or formats. Perform all necessary checks to ensure that mandatory fields are populated appropriately.
  - **KPI examples:** % of incorrect values in a dataset (error rate), % of data that is accurate, number of data points outside accepted predefined ranges.
- **Consistency:** Check for logical consistency and coherence within the data. This includes verifying relationships between data elements, identifying discrepancies, and ensuring compliance with any predefined rules or constraints.
  - **KPI examples:** number of conflicting records, % of data that complies to predefined data standards, cross-field and cross system consistency rate.
- **Integrity:** Ensure that data is free from errors, duplication, or corruption. This involves detecting and resolving data inconsistencies or conflicts. Check all data inputs for completeness, accuracy, and consistency before entering them into the system.
  - **KPI examples:** % of data duplication rates, data anomaly detection (patterns and outliners in data), consistency in relationships between tables in a database.

Data Verification

Data verification focuses on confirming the accuracy and authenticity of data by comparing it against reliable and authoritative sources. It involves cross-referencing data with trusted references or validating it through independent means. The main objectives of data verification are:

- **Source Verification:** Confirm the accuracy and reliability of data by verifying it against reliable sources, such as official documents, databases, subject matter experts or individual customers when necessary.
- **Accuracy Verification:** Perform checks or comparisons to verify the accuracy of data, ensuring that it aligns with expected values or information from reliable sources.
- **Data Integrity Verification:** Ensure the integrity of data by checking for data consistency, completeness, and adherence to predefined standards or business rules
- **Implementation and use of Automated Validation:** This includes use of data entry controls, such as format checks, range validations, and logical consistency checks, where applicable.

5. Standardised Data Formats

Standardised data formats refer to the use of consistent and predefined formats for representing and structuring data elements within a system or across different systems (Appendix Two). These formats establish a set of rules and conventions that govern how data is organised, stored, transmitted, and interpreted.

The System and Data Governance Board will be the platform for decisions relating to the standardised data format below:

- **Consistency and Interoperability:** ensuring consistency in how data is represented and interpreted across different systems, applications, or platforms. This promotes interoperability and seamless data exchange between systems, allowing for efficient integration and data sharing.
- **Data Integrity and Accuracy:** defining specific data formats throughout the system, such as field lengths, data types (text, numeric, date), and formats (e.g., date formats like dd/mm/yyyy), helps to maintain data integrity and accuracy. They prevent data entry errors, ensure data is stored and transmitted correctly, and reduce the risk of data corruption or misinterpretation.
- **Data Integration and Analysis:** facilitating data integration and analysis processes. When data is consistently formatted, it becomes easier to combine and compare data from multiple sources, perform data transformations, and conduct meaningful analysis. This leads to more reliable insights and informed decision-making.
- **Efficiency and Automation:** simplifies data processing and automation tasks. With consistent formats, automated processes can be designed and implemented to manipulate, validate, and transform data efficiently. This reduces manual effort, minimises errors, and improves overall operational efficiency.
- **Reporting and Compliance:** supports reporting requirements and compliance with regulatory frameworks. Many reporting standards and frameworks mandate the use of specific data formats to ensure consistency, comparability, and transparency in reporting practices. Especially when reporting performance data to central government or senior management.

- **Data Migration and System Upgrades:** when migrating data between systems or upgrading existing systems, standardised data formats facilitate a smooth transition. Consistent formats simplify data mapping and transformation tasks, reducing the complexity and effort involved in data migration projects. Create a standardised data migration plan that is adaptable to each scenario and includes UAT, SIT and other activities.
- **Data Governance and Documentation:** contribute to effective data governance practices. They enable clear documentation of data structures, field definitions, and data relationships, promoting transparency, consistency, and understanding across the organisation.

Mandatory Fields

Mandatory fields, also known as required fields or compulsory fields, are data input fields that must be completed or populated before a form or system can be submitted or saved successfully. These fields are marked as mandatory to ensure that essential information is provided and to prevent incomplete or inaccurate data from being entered. Mandatory fields should also be formatted to a standard across all systems. E.g.: UPRN, Name, Postcode.

It is essential to strike a balance between collecting necessary information and burdening users with an excessive number of mandatory fields. Clear communication, user-friendly interfaces, and well-defined data input standards can help with the effective implementation of mandatory fields in systems.

Purpose of Mandatory Fields

- **Ensuring Completeness and Uniformity:** ensures that all necessary information is captured and consistent and no vital data is missing.
- **Data Integrity and Accuracy:** improves data quality and accuracy, reducing errors and inconsistencies.
- **Enforcing Data Standards:** promotes adherence to predefined data standards, conventions, and validation rules.

Identification of Mandatory Fields

- **Visual Indicators:** mandatory fields are typically marked with asterisks (*), labels indicating their mandatory status, or visual cues like bold or highlighted text. Appropriate error messages or prompts should be provided on screen when mandatory fields are left blank. % of errors/blank fields will be reported to SADG as part of the Data Steward auditing responsibility.
- **System Prompts:** users may receive error messages or prompts if mandatory fields are left blank when attempting to submit or save a form.
- **Documentation:** data input guidelines or accompanying instructions should identify which fields are mandatory, providing clarity to users. These should be clearly communicated to users. Ideally this should be specified when new systems are implemented.
- **Definition and maintenance:** of mandatory fields will be overseen by the Systems and Data Governance Board.

Importance of Completing Mandatory Fields

- **Data Integrity:** ensure that critical data required for accurate record-keeping, analysis, or decision-making is captured consistently. Ensure that staff understand the importance of completing all required fields accurately and promptly.
- **Business Processes:** facilitates smooth workflow processes, as missing or incomplete data can lead to delays or errors in subsequent tasks or actions
- **Regulatory Compliance:** may align with regulatory or legal requirements, ensuring the organisation captures essential information to meet compliance obligations.

Considerations for Designating Mandatory Fields

- **Relevance:** only essential fields should be designated as mandatory to avoid unnecessary activity for users and data overload
- **User Experience:** maintain a balance between data collection needs and a user-friendly experience, ensuring that mandatory fields are clearly identified and easily navigable.
- **Data Validation:** mandatory fields often accompany data validation checks to ensure the accuracy and completeness of the entered information. These should be audited by the Data Stewards.

Controlled Vocabularies and Code Lists

Controlled vocabularies and code lists are two tools used in information management and data organisation to ensure consistency and standardisation in the representation and classification of data in a system. The key difference between controlled vocabularies and code lists is the level of granularity and usage. Controlled vocabularies focus on providing standardised terms or phrases for describing concepts, while code lists focus on providing standardised codes or identifiers for specific data values

Controlled Vocabularies: refer to a predefined and limited set of terms or phrases that are used to describe or categorise information within a specific domain or context. These vocabularies should be carefully managed to ensure that the terms used to describe things are consistent, unambiguous, and widely understood. Controlled vocabularies are more suitable for text descriptions and can be used for indexing, searching, and retrieval purposes.

Code Lists: are a collection of codes or identifiers that represent specific types, categories, or values of data in a system or database. These codes are typically alphanumeric and are assigned to specific attributes or options within a dataset. Code lists are often used in databases, data exchange formats, or programming interfaces to ensure consistency in data representation and interoperability between systems.

Examples of these would be country codes or product codes etc.

It is important that each service in accordance with standards and subject to approvals from the SAD Governance Group and Application Support:

- Utilise controlled vocabularies and code lists for standardising specific fields where appropriate, such as street types, service categories, or other relevant classifications.
- Maintain and update these lists regularly to accommodate changes and new requirements.

NB: *where fields become relevant in the future for reporting purposes that are not mandatory, it will be service management responsibility to acknowledge and work with service Data Stewards and Application Support to add mandatory fields as appropriate and to provide update to users appropriately*

6. Data Ownership – Roles and Responsibilities

Data ownership should form part of service users' responsibilities (as subject matter experts) who currently have responsibility for reviewing, reporting, and/or auditing data within their service areas across all systems and data sources.

A) Data Entry/Input

- Responsible for inputting data accurately and efficiently into the system.
- Ensures that all required fields are completed according to the data input standards.
- Performs data validation checks and verifies the accuracy and completeness of entered data.
- Reports any inconsistencies, errors, or issues encountered during data entry to the relevant supervisor or manager.
- Adheres to data privacy and security protocols, ensuring the confidentiality of sensitive information.

B) Service Data Stewards (Data Custodians)/ Service Manager (Data Owners)

- Are the data owners of data sets within their service areas.
- Establishes and maintains data input standards, processes, and guidelines for their service/s area.
- Provides guidance, training, and support to staff with responsibility for data entry.
- Performs regular quality checks and audits on entered data to identify and rectify errors or inconsistencies.
- Collaborates with relevant departments to define and update data validation rules and controls.
- Monitors data input performance and identifies areas for improvement and implements necessary changes to enhance data quality.
- Ensures compliance with data protection regulations, records management and organisational data governance policies.
- Creates and updates data reports for statutory, strategic and regulatory measures on behalf of the service.
- Works and communicates with the System and Data Governance Board and Group members.

C) System Administrator

- Ensures that the data input systems and applications are configured properly to support accurate and efficient data entry.
- Maintains user roles, access controls and permissions within the systems.
- Monitors system performance and troubleshoots any technical issues related to data input.
- Collaborates with the IT Service team to implement system updates, patches, and enhancements.
- Conducts system backups and data recovery procedures to prevent data loss (undertaken by the IT Service team).
- Ensures that data sets are adequately documented, including metadata descriptions, data dictionaries, and data catalogues. This enables data users to understand the meaning, structure, and context of shared data.

D) System and Data Governance Board and System and Data Governance Group

- Board profile is Director, Assistant Director, ICT and Business Improvement.
- Group Profile is Assistant Director, ICT, Business Improvement and 4th Tier Management representation.
- Establishes, updates and embeds data strategy and policy.
- Drives a data driven culture of valuing high quality data across the organisation.
- Documents and communicates expectations and requirements to ensure data is compliant and stored, used, shared and disposed of in accordance with corporate standards and relevant legislation.
- Documents and communicates expectations and requirements across the organisation in respect of the data standards and quality
- Prioritises systems and data projects.
- Prioritises the enablement for data initiatives and automation.
- Drives data literacy, training and development throughout the organisation to enhance the workforce data and analytical skills.
- Oversees the procurement of new systems.

E) Assistant Directors

Are accountable for the accuracy and quality of performance data and information within their service area.

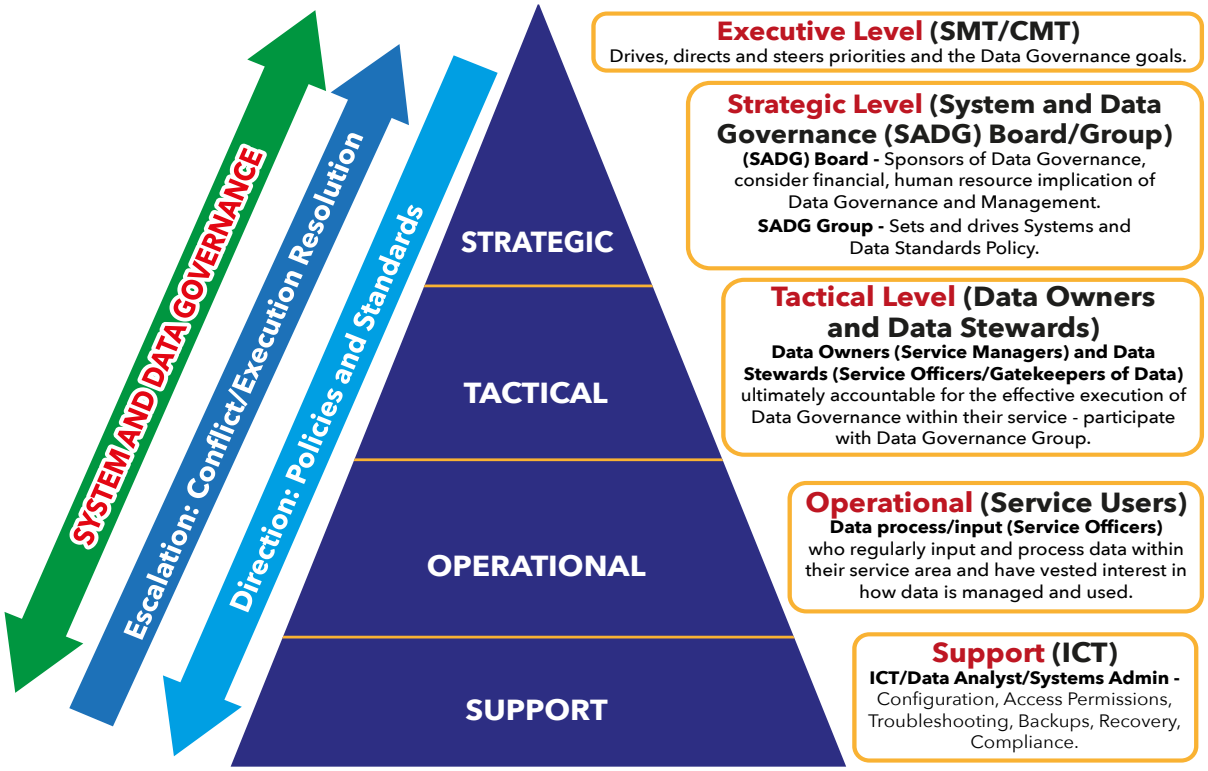
F) Senior Management Team/Directors

Has overall responsibility for challenging performance and data quality.

The above roles and responsibilities provide a general framework and it is recommended to adapt and refine them based on service specific needs and the wider organisational context.

G) All Employees

Responsible for adhering to data privacy and security protocols, ensuring the confidentiality of sensitive information.



7. Data Sharing and Interoperability

Data sharing and interoperability refers to the principles and practices that enable the exchange and compatibility of data between different systems, departments, and organisations within the local government environment.

Data sharing involves the intentional and controlled sharing of data between various stakeholders, such as government agencies, departments, or external organisations, to enhance collaboration, decision-making, and service delivery.

Interoperability focuses on ensuring that different systems, databases or applications can work together seamlessly and exchange data effectively. It involves the use of common standards, protocols, and formats to enable data compatibility and integration across various platforms or entities. Interoperability allows different systems to understand and utilise shared data without data loss, misinterpretation, or technical barriers.

This policy provides guidelines and rules for data sharing and interoperability. It requires the organisation to have these elements in place:

- **Data Governance:** Implement governance mechanisms to manage data quality, accuracy, security and privacy throughout its lifecycle. This includes data stewardship, data validation processes and data sharing agreements.
- **Data Access and Permissions:** Clearly define who can access and share data, including roles, responsibilities and authorisation processes. It ensures that data sharing is done in accordance with privacy and data protection regulations.
- **Data Standards:** Establish common data standards, formats, and classifications to ensure consistency and compatibility across different systems. This enables data from diverse sources to be integrated and analysed effectively.
- **Technical Infrastructure:** Develop and utilise interoperable systems, software, and technologies that support seamless data exchange and integration. This may involve adopting open standards, application programming interfaces (APIs) and data integration platforms.
- **Metadata and Documentation:** Ensure that data sets are adequately documented, including metadata descriptions, data dictionaries, and data catalogues. This enables data users to understand the meaning, structure, and context of shared data.
- **Uniqueness:** Ensure data items in a dataset are distinct from one another and represents a unique piece of information.
- **Collaboration and Partnerships:** Encourage collaboration and partnerships with external stakeholders, such as other government agencies/authorities, non-profits, or private organisations. This promotes data sharing and interoperability beyond the local government boundaries, leading to enhanced insights and improved public services.

Data sharing and interoperability supports a culture of collaboration, innovation, and evidence-based decision-making. It will enable the organisation to leverage data assets effectively, improve service delivery and address complex challenges by harnessing the collective power of data from multiple sources.

8. Data Retention and Disposal

Data retention and disposal refers to the process of managing and controlling the lifespan of data held by the council in accordance with the data retention and disposal schedules.

Data Retention: the purpose of data retention is to ensure that the council does not retain data past its retention period to meet its legal, regulatory, and operational requirements. Distinct types of data may have different retention periods based on the nature of the information and applicable laws or regulations. For example, financial records may need to be retained for a longer duration than general correspondence.

The data retention schedule defines the retention periods for distinct categories of data, specifying the minimum duration for which data must be retained. Once the retention period for specific data has expired, services need to initiate the disposal process.

As part of the accountability principle, all systems should have a retention and disposal policy built in, with a trigger to assist with compliance.

Data Disposal: involves permanently deleting, destroying, or anonymising data to ensure it cannot be accessed or retrieved by unauthorised individuals. Disposal methods should comply with applicable privacy and data protection laws to prevent any unauthorised access, disclosure, or misuse of information.

The data disposal process should be carefully planned and executed, ensuring that all copies or backups of the data are appropriately removed or destroyed. Depending on the sensitivity of the data, disposal methods may include physical destruction of storage media or secure deletion of digital files.

It is essential that all services adhere to these schedules to ensure compliance with relevant laws, protect individual privacy, and minimise the risks associated with retaining unnecessary or outdated data.

Data Access and Transparency

Data access and transparency in the council refers to the principles and practices that govern how data is made available to authorised individuals or entities, and how the council ensures openness and accountability in its data management processes.

Data Access: refers to the ability of authorised individuals or groups to retrieve, view and use the council's data. Access controls and permissions should be implemented to ensure that only authorised personnel can access sensitive or confidential information. This helps protect privacy, prevent data breaches and maintain the integrity of the council's data assets.

Transparency: refers to the council's commitment to openness and accountability in its data management practices. It involves providing clear information about the council's data holdings, data collection processes and how the data is used. The council should state its commitment to transparency and its intent to make relevant data available to the public, subject to privacy and security considerations.

To ensure transparency, the council should include provisions for publishing datasets that are non-sensitive, non-confidential and in the public interest. This can be achieved through the creation of customer portals where customers can access their own data alongside other approved datasets.

While transparency is a stated aim, it is important to ensure that published data is done in accordance with data protection. It is vital that openness and accessibility is balanced with the protection of sensitive information and individual privacy rights.

By undertaking to share its data in a safe and legal way the council can foster an environment of accountability, public trust and greater engagement. It can enhance collaboration, support evidence-based decision-making and encourage innovation through the responsible and ethical use of its data.

9. Data Privacy and Security

Data privacy and security are crucial aspects of protecting sensitive information from unauthorised access, use, disclosure, alteration or destruction.

Data Privacy: refers to the right of individuals to have control over their personal information and how it is collected, used, and shared. It involves safeguarding personal data from being accessed or used in ways that are inconsistent with the individual's consent or legal requirements. Data privacy regulations, such as UK GDPR outline the obligations of organisations when handling personal data, including obtaining consent, transparency, and ensuring individuals' data rights are maintained.

Data Security: focuses on protecting data from unauthorised access, loss, or damage. It involves implementing measures to ensure the confidentiality, integrity, and availability of data. This includes employing technical and organisational safeguards, such as encryption, access controls, firewalls, security audits, and cyber security to prevent data breaches and unauthorised access.

Both are crucial in maintaining the confidentiality and trustworthiness of sensitive data. Consequently, it is vital that services

- Comply with all relevant data protection regulations, including the UK GDPR, when inputting personal data.
- Obtain necessary consent and ensure the appropriate level of data anonymisation or pseudonymisation are in place.
- Adhere to established data security policies and practices to protect sensitive information from unauthorised access or disclosure.

10. Training

All Employees:

Training is crucial for ensuring good data input and governance across the organisation. Training provides individuals with the necessary knowledge and skills to effectively handle data, understand data governance policies and follow established processes. It equips employees with the expertise to accurately capture, validate and enter data into systems, minimising errors and ensuring data quality. Regular training can help to foster a culture of data compliance and risk mitigation.

- Ensure a comprehensive training plan is provided to all staff members involved in data input, emphasising the importance of accurate and validated data. Especially when new systems are implemented.
- Ensure ongoing access to resources, such as user manuals, policies and standards, to address questions or issues related to data input.
- All staff accessing our Council systems currently must complete information Security Policy training, data protection training and Cyber security training.

Data Stewards:

Specific, tailored training programmes will be developed for the Service Data Stewards aligning to their roles and responsibilities for data stewardship, auditing and analytical reporting. The System and Data Governance Board and Group will work closely with the Human Resource team and Service Managers to review skills and competencies and agree and develop appropriate and timely training provision.

Appendix One

Data Input Standards, Processes, and Guidelines

Effective data input is crucial for maintaining accurate and consistent information within our systems. This Appendix outlines the data input standards, processes, and guidelines to ensure staff have a reference point for accurate and consistent data entry. Adhering to these standards will help maintain data integrity and enhance the quality of our organisational data.

1. Data Input Standards

1.1. Accuracy

- Input data accurately, ensuring that information is entered as intended and without errors.
- Double-check data entries for accuracy before submitting or saving them.

1.2. Completeness

- Fill in all required fields, ensuring that no essential information is left blank.
- Avoid leaving optional fields empty when relevant information is available.

1.3. Consistency

- Follow standardised formats, conventions, and terminology as specified for each data field.
- Use consistent abbreviations, spellings, and capitalisation throughout the data entry process.

1.4. Validity

Validate data against reliable sources, such as official documents or authorised databases e.g. the NLPG for address data etc. Implement and adhere to national standards such as BS7666 Data Standards.

BS 7666 is a standard that provides guidelines for organising and managing information about addresses and geographic locations. It helps to make sure that addresses are recorded and presented in a uniform and structured manner. It defines how different elements of an address should be arranged, such as the house number, street name, city, and postal code. By following these guidelines, it becomes easier to store, exchange and compare address data across different systems and databases.

BS 7666 also covers geographic locations, like points of interest, landmarks, and boundaries. It establishes a common framework for identifying and describing these places, which helps in mapping and navigation systems

- Perform necessary checks to ensure data entered meets predefined validation rules and criteria.

2. Data Input Processes

2.1. Familiarise Yourself with Input Screens/Forms and the System

- Understand the purpose and structure of the data input screens/forms or system before entering data.
- Review any accompanying instructions or guidelines to ensure accurate data entry.

2.2. Verify and Validate Data

- Validate data against relevant sources to ensure accuracy and completeness.
- Cross-check data against existing records to avoid duplicates or conflicting information.

2.3. Follow User Level Guidance

- Refer to user guidance or tooltips provided within the data input screens/forms or system.
- Ensure that the correct data type, format, and length are used for each field.

2.4. Review and Edit

- Review the entered data for accuracy, completeness, and consistency.
- Make necessary edits or corrections before finalising the data entry.

2.5. Seek Clarification

Seek assistance or clarification from managers, supervisors or colleagues when encountering ambiguous or complex data.

3. Additional Guidelines

3.1. Data Privacy and Security

- Adhere to data protection regulations, including obtaining necessary consent and protecting personal information.
- Use secure login credentials and follow security protocols when accessing data input systems.

3.2. Timeliness

- Enter data promptly to ensure that information is up to date and relevant.
- Avoid unnecessary delays in data entry to maintain the accuracy and usefulness of the data.

3.3. Documentation

- Maintain appropriate records or documentation related to data sources, validation processes, or any changes made during data entry.
- Document any issues, errors, or discrepancies encountered during the data input process.

4. Training

- Attend training sessions or workshops to enhance data skills and knowledge.
- Seek assistance from managers, supervisors and administrators when encountering challenges or uncertainties during data entry.

Appendix Two

Common Data Fields and Formats

The most common data fields in use across all our systems are:

- Title (Mr, Mrs, Ms, Dr, Prof etc)
- Name (First, Middle, Surname)
- Unique Property Reference Number (UPRN)
- Address (Line 1, Line 2, Line 3, Line 4, Postcode)
- Date of birth (dd/mm/yyyy)
- Customer Recognition Number
- Contact telephone number
- Email address

Whilst this data is routinely captured in our systems, it must be done so consistently, following the same formats across as many of our systems as possible. (See table below)

Address data should be held as BS7666 standard format (See Appendix One)

The Unique Property Reference Number (UPRN) should also be used across the councils' systems.

Standardised Format	
Item	**Item Description**
System	What is the Software System
Standard Field Name	Field name (eg: First name, Surname, Address line 1 etc)
Definition	What is this used for eg: UPRN a reference for address location
Key Identifier/ Primary Key	Is this field a Primary Key or Key Identifier eg: Name, CRN, Address, Postcode, UPRN, Telephone, Email
Data Type	AutoNumber, input number, long / short integer, text, date
Format	What characters accepted/standards - set characters, variable characters, case sensitive, full details, part details, abbreviations
Validation	What validation is set for this field eg: how data is inputted, is it automated or manually inputted, is there restricted input/choice, lookup, prefixes, no of spaces etc.
Mandatory Field	Yes or No (must be completed or automated or unable to move to next etc)
Character Length	Max no of characters
Based on/Source	What is the standard / where has the data derived from (eg: UPRN from GeoPlace - Ordinance Survey)
Verification	Is this assigned field? - eg: UPRN is assigned based on address and not manual entry
Comments	Why is it important - is it used to integrate, index, access through a Portal, report etc.
Version	Updates
Approval Date	SADG sign off date

Appendix Three

Summary Document - Data Standards Policy

1. Introduction

This summary document outlines the details of our Data Standards Policy and is designed to ensure consistency, transparency, and security in the handling of data across all service areas. The policy aims to establish a framework that supports efficient data management, sharing, and usage while complying with relevant legal and regulatory requirements.

2. Scope

This policy summary document applies to all data collected, stored, processed, shared, and disposed of by council employees, including data from external partners, contractors, and service providers. It covers both structured and unstructured data across all formats, including digital and physical records.

3. Data Governance

Data governance and documentation are vital in today's connected data-driven world. Effective data governance helps the organisation to maximise the value of its data, mitigate risks, and comply with regulatory requirements.

A System and Data (SAD) Governance Board has been established to provide governance for the overall management, control, and protection of the organisation's data assets. The Board will be responsible for establishing strategies, policies, processes, standards and guidelines to ensure the proper collection, storage, usage, and sharing of data. The SAD Board aims to promote and provide support on data quality, consistency, integrity and security across the organisation by:

- **Key Service Roles and Responsibilities:** Establishing clearly defined roles for data governance, including Data Owners, Data Stewards, and Data Users, with specified responsibilities for data management, quality, reporting and security.
- **Data Management Plan:** Each service area must have a data management plan outlining how data is collected, stored, processed, and disposed of in accordance with this policy summary document.
- **Data Lifecycle:** Data should be managed through its entire lifecycle, from creation and usage to archiving and deletion, in line with legal requirements and retention schedules.

4. Objectives

- **Consistency:** Ensure uniform data formats, structures, and processes across all service areas to facilitate seamless integration and interoperability.
- **Transparency:** Enable clear and accessible data records to promote accountability and public trust.
- **Security:** Protect data from unauthorised access, breaches, and misuse, ensuring compliance with data protection laws.
- **Efficiency:** Optimise data handling processes to reduce redundancy, improve accuracy and support decision-making.
- **Compliance:** Adhere to all relevant legislation, including the Data Protection Act 2018, GDPR and Freedom of Information Act 2000.

5. Data Classification

Data must be classified according to its sensitivity and criticality, as follows:

- **Public:** Data that can be freely shared with the public, e.g., public service information.
- **Internal:** Data intended for use within the local government, e.g., internal memos, routine administrative data.
- **Confidential:** Data that should only be accessible to authorized personnel, e.g., personal data, financial records.
- **Restricted:** Highly sensitive data requiring strict access controls, e.g., national security-related information.

6. Data Quality

All data should meet the following quality criteria:

- **Accuracy:** Data must be correct and reflect reality.
- **Completeness:** All necessary data elements must be captured.
- **Consistency:** Data should be consistent across all systems and formats.
- **Timeliness:** Data must be up-to-date and available when needed.
- **Validity:** Data must conform to established and agreed formats and standards.
- **Uniqueness:** Duplicate records should be minimised and managed appropriately to create a 'single version of the truth'.

7. Data Standards

- **Metadata:** All datasets must include metadata that describes the data's source, date of creation, update history, format, and any relevant classifications. (these will be owned by each service area).
- **Data Formats:** Data should be stored in open, non-proprietary formats wherever possible (e.g., CSV, JSON, XML) to ensure long-term accessibility and interoperability.
- **Standardise Naming Conventions:** Standardised naming conventions must be used for files, databases, and field names to ensure clarity and consistency.
- **Data Models:** Common data models should be adopted across all services to enable interoperability and data sharing.
- **BS 7666 standard** should be adhered to and is a standard that provides guidelines for organising and managing information about addresses and geographic locations. It helps ensure addresses are recorded and presented in a uniform and structured manner. It defines how different elements of an address should be arranged, such as the house number, street name, city, and postal code. By following these guidelines, it becomes easier to store, exchange, and compare address data across different systems and databases.

8. Data Security

- **Access Control:** Implement role-based access controls to ensure that data is only accessible to authorised individuals.
- **Encryption:** Sensitive data must be encrypted both at rest and in transit to prevent unauthorised access.
- **Incident Management:** Establish procedures for reporting, responding to, and mitigating data breaches or other security incidents.
- **Auditing:** Regularly audit data processes and access logs to ensure compliance with security protocols.

9. Data Sharing

- **Inter-Governmental Sharing:** Establish protocols for securely sharing data between local government bodies, including data sharing agreements that define the terms and conditions of use.
- **Public Access:** Data intended for public access should be published in open data formats and made available through appropriate channels, subject to confidentiality and privacy considerations.
- **Third-Party Sharing:** Any data sharing with third parties must be governed by formal agreements that specify data protection, usage and security requirements.

10. Compliance and Monitoring

- **Legal Compliance:** Ensure all data handling practices comply with the Data Protection Act 2018, GDPR, and other relevant legislation.
- **Monitoring and Auditing:** Regularly review data processes, security measures and compliance with this policy summary document. Audits should be conducted annually or as needed.
- **Training:** Provide regular training for all employees on data standards, security practices, and their roles in ensuring compliance.
- **Tailored Training:** provide tailored training for data stewards and analysts to support auditing, reporting and standardisation.

11. Review and Update

This policy summary document should be reviewed and updated annually or whenever there is a significant change in relevant legislation, technology, or organizational structure.

12. Exceptions

Any exceptions to this policy summary document must be formally documented, justified and approved by the relevant authority (SAD Board) with a clear plan for mitigating any associated risks.

13. Consequences of Non-Compliance

Non-compliance with this policy summary document may result in disciplinary action, including potential legal ramifications, depending on the severity of the breach.

This policy serves as a summary guide for managing data within the organisation and supports the full Data Standards Policy.

Version Control				
Title		Data Standards Policy		
Description		To support the delivery of Customer & Digital Strategy 2020-2026 in relation to improving and aligning data		
Created by		Business Improvement Team, Business Transformation, Organisational Development and Digital Strategy Directorate		
Date created		January 2025		
Maintained by		Business Improvement Team		
Next Review Date		March 2026 (Aligned to Customer and Digital Strategy 2020 - 2026)		
Version number	**Modified by**	**Modifications made**	**Date modified**	**Status**
1				