Data Management Policy 2025 - 2028

Creator	Author(s)	Ann-Marie Johnstone (Head of Governance, Policy and Information); Victoria Holmes (Data & Analytics Manager).
	Approved by	Leanne Hamer (Governance & Information Manager)
	Department	Legal and Governance Services
	Service area	Governance, Policy and Information
	Head of Service	Ann-Marie Johnstone
	Director	Charlotte Benjamin
Date	Created	2022/09/23
	Submitted	2025/10/15
	Approved	TBD – planned for 20251218
	Updating Frequency	3 years
Status	Version: 2	
Contributor(s)	Head of Governance, Policy and Information and SIRO; Governance and Information Manager; Data Protection Officer; Data and Analytics Manager.	
Subject	Data management; statutory returns;	
Type	Policy	
	Vital Record	EIR
Coverage	Middlesbrough Council	
Language	English	

Document Control

Version	Date	Revision History	Reviser
0.1	20190530	First draft	V Holmes
0.2	20190910	First revision	AM Johnstone
1.0	20191115	Finalised	P Stephens
1.1	20210316	Data classification approach added	L Hamer
1.2	20221130	Social Care Policy update	M Brearley
2.0	20251014	Second Draft Revision	V Holmes

Distribution List

Version	Date	Name/Service area	Action
1.0	20191130	WLMT	Implement
1.1	20210430	All staff via Intranet	Implement
1.2	20221130	All staff via Intranet	Implement
2.0	20260101	All staff via Intranet	Implement

Contact:	data@middlesbrough.gov.uk

Summary

This policy is part of the framework underpinning the Council's Information Strategy, and sets out how the Council will effectively standardise, manage, link and exploit data throughout its lifecycle, and ensure that it meets its obligations in respect of data integrity, statutory returns to Government, statutory information requests and data transparency.

The following sections outline:

- the purpose of this policy;
- definitions;
- scope;
- the legislative and regulatory framework;
- policy statement;
- roles and responsibilities;
- supporting policies, procedures and standards; and
- monitoring and review arrangements.

Purpose

The purpose of this policy is ensure a systematic approach to data management across the data lifecycle, across the organisation, to support the vision set out in the Information Strategy that 'the right information will be available to the right users, at any time, accessible and used ethically to support achievement of the Council Plan.'

This policy will ensure that the data it holds is:

- accurate, complete, timely, relevant, reliable, valid and available
- standardised and linkable where possible
- explained where appropriate to ensure that it is not misused in error
- stored securely and in a manner that protects confidentiality and integrity
- securely disposed of in line with the Council's Retention Schedule.

Compliance with this policy will deliver the following benefits:

- improved integrity, availability and sharing of data
- improved understanding of citizen and customer needs
- better and more timely decision-making and improved value for money
- ensuring good data quality will increase the Council's opportunities to automate processes through use of Artificial Intelligence. This can add value and improve outcomes
- ensure good data quality will support accurate forecasting through predictive analytics across Directorates.

It will also help the Council to mitigate the following risks:

- loss of data due to a lack of security
- data breach of sensitive information, either personal or commercial
- poor decision making or failure to act due to data shortcomings
- poor decision making due to poor data quality used in predictive analytics.

Definitions

Data management	The process for acquiring, validating, storing, protecting, and processing required data to ensure its security, confidentiality, integrity and availability for users and requesters.
Data integrity standard	The standard to which data sets will be maintained to ensure they meet required integrity standards (e.g. the level of completeness, accuracy, timeliness etc. required).
Data processing standard	The standard of processing to be maintained to ensure that data meets the integrity standard.
Digital continuity	The ability to access and maintain digital data throughout its lifecycle regardless of the system it is held on. Digital continuity should be ensured in the commissioning of a new system to avoid data loss or interruption through the extraction and migration of data the new system or an appropriate archiving solution.
Information	Refers to: (unstructured) data, (structured) information, and records (of interactions, policies or decisions). The Council holds information in many different formats; in physical and digital form, both online and offline; on premises and externally.
Golden record	A single, well-defined source of data for certain data points e.g. date of birth, address.
Records	Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Information security	Organisational and technical measures that are put in place to prevent security incidents that could affect the confidentiality, integrity, or availability of personal data.
Information classification	How the Council will classify information assets to ensure they are appropriately protected.
Data disposal	The process for ensuring data is securely disposed of and appropriately recorded once its retention period has passed.
Master Data Management	The method used to define and manage the critical data of an organisation to provide, via data integration, a single authoritative points of reference for e.g. customer, asset or spatial data.
Data anonymization	The process of rendering personal data anonymous in such a manner that the data subject is not or no longer identifiable.
Data pseudonymisation	The de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

Data lifecycle	Data lives through six stages – creation; organisation; access and use; maintenance; archiving and preservation and destruction. The life period of data is determined by the Council’s Retention Schedule.
Personal data accuracy	Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Privacy by design	The legally required steps taken to integrate appropriate technical and organisational measures, from the design stage, to implement the data protection principles and safeguard individual rights with DPIAs being completed where necessary e.g. new purpose for existing data.
Smart data model	This standardised, interoperable data structures that define how real-world entities and concepts are digitally represented for consistent data sharing and integration.
Customer data	Data refers to any information relating to a customer’s interactions with a trader, including details about supplied goods, services, or digital content, pricing, usage, and performance.
Business data	Data refers to any information about a trader’s goods, services, or digital content, including details of their supply and customer feedback

Scope

This policy applies to all employees (both permanent and temporary), contractors and consultants of the Council who are given the authority to create, access, maintain or dispose of Council data.

It applies to all data created and /or maintained by the Council, whether created or received and managed directly, or by third parties on its behalf. It also applies to data created, received or managed by the Council in partnership with, or on behalf of, other organisations.

Legislative and regulatory framework

Key elements of the legislative and regulatory framework for data management are set out below. Failure to comply with this framework can lead to significant financial penalties, criminal prosecution and non-criminal enforcement action.

UK General Data Protection Regulation 2016 (UK GDPR), Data Protection Act (DPA) 2018	GDPR and the DPA places a duty on the Council to manage personal data in a way that complies with the data protection principles: lawfulness, fairness and transparency, purpose limitation, data minimisation,

	accuracy, storage limitation, integrity and confidentiality (security), and accountability. It also obliges the Council to respond to requests from individuals to exercise their data protection rights where these apply including the rights: to be informed, of access, to rectification, to erasure, to restrict processing, to data portability, to object, or relating to automated decision-making and profiling.
Data (Use and Access) Act 2025 (DUAA)	Updates some areas of data protection law and adds new functions including Digital Verification Services, National Underground Asset Register, Digitising Registers of Births and Deaths, and Online Data Processing.
Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (PECR)	PECR regulates the privacy rights of individuals relating to electronic communications including: marketing calls, emails, texts and faxes; cookies (and similar technologies); keeping communications services secure; and customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.
Digital Economy Act 2017	Provides government powers to share personal information across organisational boundaries to improve public services.
Environmental Information Regulations 2004 (EIR)	Deriving from European law, this provides for public access to ‘environmental information’ held by public authorities, unless specific exception(s) apply. It is also obliged to proactively and routinely publish information that has been frequently requested in the past in its Publication Scheme.
Freedom of Information Act (FOIA) 2000	Under the FOIA, the Council has a duty to make information available to the public upon request, unless specific exemption(s) apply. It is also obliged to proactively and routinely publish information that has been frequently requested in the past in its Publication Scheme. Poor data quality would hinder the amount of information the Council could publish.
Local Government Acts 1972, 1985, 1988 and 1992	Establishes requirements to manage records and information, and requires councils to use data to make informed decisions to ensure value for money and compliance with a range of statutory duties.
Local Government Transparency Code 2015	Requires local authorities to publish certain information, specifying content and frequency of publication, and recommends the publication of certain other information.
Lord Chancellor’s Code of Practice on handling information requests	Issued under s.45 of the FOIA, the code sets out the practices which public authorities should follow when dealing with requests for information under the Act.

Other Regulations and Codes of Practice	The Council's approach is also informed by range of other regulations and codes of practice, including: • ISO 15489 Records Management; • Lord Chancellor's Code of Practice on the management of records; • National Data Guardian's Data Security Standards; • Requirements for statutory data returns to Government departments; • Re-use of Public Sector Information Regulations 2005; • 'Caldicott principles' on NHS patient information (revised 2013) and the NHS Data and Protection Toolkit; • National Data Opt-Out in Health and Social Care • ONS Code of Practice for statistics (voluntary application); • Open Standards Principles; and • Information Commissioner's Office (ICO) Data Sharing Code of Practice (forthcoming). • ICO Anonymisation Guidance

Policy detail

The Data and Analytics Team will work collaboratively with Information Asset Owners, Information System Owners and other key personnel to optimise the performance of its data, ensuring that it is of the appropriate quality and integrity, is easily accessible and works smoothly.

This work will ensure that the Council's datasets are of the right standard support evidence-based approaches to strategy, policy and commissioning and so effectively support the delivery of its strategic objectives. Data gaps identified by this work will be progressed in line with the Council's priorities.

Data will be developed in standardised and linkable formats (e.g. 5-star Open Data) to support transparency and reuse. Where appropriate, each data item (e.g. case files) will be allocated a core Unique Reference Number (URN), where possible standardised national numbers such as National Insurance or NHS numbers to support the development of golden records, master data management and ultimately improved intelligence.

Business Intelligence dashboards will be made available for all services, and routinely used to manage service performance, drive data improvements, forecast future events via Predictive Analytics utilising Predictive Analytics Standard including Python Code and drive day-to-day decision-making. These automated data products rely on accurate data and therefore data quality will be a core consideration when developing future data products.

Equality and Inclusion must meet our data quality standards as inaccurate data can result in unfair actions and outcomes for individuals. Adherence to this policy will support the

Council to be able to implement innovative, automated uses for data that will be heavily reliant on data being timely and accurate in order to be able to automate its use effectively.

In order to support Business Continuity, the Data & Analytics team will scope (in conjunction with Service areas) data extracts that will enable continuation of operational duties in the event of cyber outage.

The Council will develop and implement solutions to support the digitisation and integration of all appropriate datasets, implementation of master data management, data harvesting and data archiving.

Source data will be held securely, with extra security measures in place for personal data. Where data is required to be analysed or shared in a raw format for internal and external parties, a privacy by design approach will be taken with data provided in anonymised or pseudonymised form.

Personal data will only be provided in fully identifiable form where this complies with data protection principles and rights. Appropriate records will be maintained of personal data shared with other agencies.

Within the legal and regulatory framework set out below, the Council will develop a ‘by default’ and, where possible, automated approach to data sharing with our partners and contractors, to support collaborative planning, commissioning and service design.

The Council’s Data Protection Officer will provide advice and guidance on all such matters as required.

Roles and responsibilities

Effective records management is the collective responsibility of all those individuals named within the scope of this policy.

Senior Information Risk Owner (SIRO)	Responsible for the overall management of information risk within the Council, advising the Chief Executive, management team and Information Asset Owners, and ensuring that staff training is available and fit-for-purpose. The role is undertaken by the Head of Governance, Policy and Information, who is also responsible for the Information Strategy. Responsible for ensuring that data integrity and availability issues are raised with Information Asset Owners and System Owners to address.
Data & Analytics Manager	Responsible for the development and implementation of the Council’s data management policy and supporting procedures, to ensure that the Council meets its obligations in respect of data integrity, statutory returns to the Government and data transparency. This policy gives the Data Manager a mandate to drive work necessary to comply with the standards set in this policy

	which are necessary to deliver the ambitions of the Information Strategy. Also, a key user of products from the Data Team. Responsible for ensuring that data used within business intelligence products complies with the standards required by this policy. Responsible for the delivery of predictive analytics products, to enable it to accurately predict future service demand to improve service planning and inform its preventative services, which will be designed to reduce demand for more intensive interventions by supporting people at an earlier stage. To facilitate Business Continuity across the council, by providing data extracts to support service areas during cyber outage.
Records Manager	Responsible for the development and implementation of the Records Management policy and supporting procedures, which will complement this policy. Providing advice and checking compliance to ensure the Council's records and well-kept and that the systems used to hold them are fit-for-purpose. The Records Manager owns the ECMS and mail and print contracts and is responsible for inactive records where an information asset owner cannot be identified.
Data Protection Officer	Responsible for assisting the council to monitor internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs), and acting as a contact point for data subjects and the supervisory authority.
Information System Owner	All information systems within the Council have an assigned owner. System owners are responsible for the security, confidentiality, integrity of availability of the information within the system and work alongside ICT, Information Asset Owners and Information Asset Assistants to implement appropriate processes and procedures to ensure agreed standards are achieved and maintained.
Information Asset Owner	Responsible for maintaining comprehensive and accurate information asset registers (IARs) for their service areas, and ensuring that: • staff in their service area are aware of their responsibilities and appropriately trained; • data and records are managed in line with the Council's policy and procedures; • information is released in line with legal requirements and this policy; and • identifying and escalating information risks to the SIRO.

Information Asset Administrators	Information Asset Administrators (IAAs) support IAOs in the good governance of information and managing information risks. IAAs will include all managers and supervisory staff and other staff with specific roles relating to the security, confidentiality, integrity and / or availability of information.
Senior System users	Senior system users (‘super users’) support the Information System Owner and, working with frontline users, are responsible for ensuring data is managed in line with this policy and supporting procedures.
All managers	Responsible for overseeing day-to-day compliance with this policy by their staff and other personnel they manage.
All staff, contractors, consultants, interns and any other interim or third parties	Responsible for creating, accessing, using and managing data and intelligence in accordance with this policy and its supporting procedures.
Information Strategy Group	Operational group of key officers led by the SIRO responsible for implementing the Information Strategy, in conjunction with Information Asset Owners.
Risk Management Group	The group ensures the Council has a suitable risk management framework in place, provides a mechanism for risk management issues to be discussed and ensures the delivery of the Risk Improvement Plan

Supporting policies, procedures and standards

The following policies, procedures and standards will be implemented across the Council to ensure that the Council’s data is managed effectively.

Data standardisation framework	Outlines procedures to enable the Council to standardise datasets and allow data to be effectively utilised, including data minimization.
Data Protection Policy	Sets out how the Council complies with data protection legislation.
Digital Communications Policy	This policy is part of the framework underpinning the Council’s Information Strategy, and sets out how the Council will ensure that its 365 email system is operated in line with the principles of effective information governance. It also places email usage within the context of the Council’s Digital Strategy.
ECMS procedures	Sets out business rules in respect of the use of the Council’s Enterprise Content Management System as the proper tool for the storage and referencing of digital records.
Public Information and Information Requests Policy	This establishes the corporate framework for responding to statutory information requests, and to proactively identify information to be routinely published using Open Standards and

	to meet the Council's requirements under the transparency code.
Records Management Policy	Sets out how the Council will manage its records to ensure they are digitized where appropriate, held securely and deleted when retention periods are reached.
Records Retention Schedule	This defines how long different records should be retained to comply with legal, regulatory or other requirements and the proper arrangements for archiving and destruction.
Sensitivity Labels	This guidance covers the rules when applying sensitivity labels to your content and applies across OneDrive, SharePoint and email. By applying sensitivity labels to this content it ensures that we keep our information secure by stating how sensitive certain information is within MBC.
Vital Records Standards	This sets out how vital records will be identified and the steps to be taken to ensure their protection and preservation.
Business Continuity Plans	These identify those vital records required to support delivery of critical services.
Disaster Recovery Plan	This identifies priorities and recovery timescales for access to ICT systems and digital records in the context of business continuity.
Predictive Analytics Standard	This document sets out the essential factors and critical information to consider when developing predictive analytics (including Python Code of Conduct) that supports strategic decision-making
AI Policy (in development)	Development of AI Policy is underway which will sets out Middlesbrough Council's framework for the lawful, ethical, and effective use of AI to improve productivity, protect personal data, and assure residents, staff, and businesses that AI is used responsibly and safely as part of its Information Governance and Digital Strategy.

Monitoring and review arrangements

The implementation and effectiveness of this policy and its supporting procedures will be overseen by the Information Strategy group which is delivering the detailed delivery plan for the strategy. That plan includes actions to improve data quality.

This policy will be reviewed every three years, unless there is significant development that would require a more urgent review e.g. new legislation.