Corporate Data Quality Policy

Author	Version	Date of last review	Date of next review
Corporate Policy and Performance Manager	v 4	April 2023	April 2026

Corporate Data Quality Policy

1. Purpose

1.1 The purpose of this policy is to help improve the quality of data collected and used by both the council and its partners. The policy helps ensure data quality is fully embedded across all services and is always a key consideration when collecting, processing or using data to support decision-making.

2. Introduction

2.1 Data quality relates to the accuracy of information used inform operational or strategic business decisions or to judge performance. Producing data that is fit for purpose is an integral part of an organisation's business processes.

2.2 Poor data quality can have many consequences. It can undermine accountability and damage public trust, weaken frontline service delivery, cost money, put vulnerable people at risk, and undermine partnership working.

2.3 Durham County Council is committed to high standards of data quality. The council recognises the importance of reliable information to support decision making at all levels. Good quality, accurate and timely data enables us to deliver and manage services, improve performance, and benefit residents and service users.

2.4 This policy sets out our approach to the management of data quality to support decision-making and compliance with relevant regulatory frameworks (See Appendix A). It is one of a suite of council policies that have been implemented to ensure that the council's data is of high quality and is maintained effectively. This includes:

- CCTV Policy and Code of Practice.pdf
- Data Protection Policy.pdf
- Data Protection Potential Breach Policy.docx
- Duty of Confidence.pdf
    - Application to access Children and Young People's Services and Adult and Health Services information by non-service staff (SS109).pdf
    - Confidentiality Agreement (SS432).docx
- Personal Information Security Policy

2.5 This policy is supported by procedures for data collection, processing and storage and calculation of outturn data used to support decision making. These procedures are reviewed and updated regularly (at least annually). These procedures will include specific arrangements for ensuring data quality at the point of collection, during the processing of that data, and appropriate data quality checks before data is used for reporting and decision making.

3. What makes good quality data?

3.1 Producing robust data is an integral part of providing strategic or operational insight, performance management and customer/public insight. Key characteristics of good quality data are:

- **Accurate.** Data should be sufficiently accurate for its intended purposes. Data should be captured only once (although it can have multiple uses) and as close to the point of activity as possible. Its importance should be balanced with the costs and effort of collection. If accuracy is compromised, the resulting limitations should be made clear when data is reported.

- **Secure.** Information is stored safely and with appropriate access controls. Sensitive information is only used for the purpose it was collected, and only retained for as long as it is needed. Information is only shared with others where the council is satisfied that appropriate controls and safeguards are in place. Access to and use of data should be appropriate to the data user and comply with relevant legislation such as the General Data Protection Regulation (GDPR.)

- **Valid.** Data should be recorded in an agreed format and should comply with recognised council and national standards. Where proxy data is used to compensate for the absence of actual data, it must be considered how well this data is able to satisfy the intended purpose and the appropriate warning reported alongside data being reported to ensure transparency. Validity checks should be carried out before reporting data.

- **Reliable.** Data should reflect stable and consistent data collection processes across the council. Reported data should conform to documented definitions and be collected and calculated in accordance with the documented methodology and procedures.

- **Timely** - Data should be available within a reasonable timescale, and quickly and frequently enough to support information needs and effective decision making.

- **Relevant** - Data should be relevant to the purposes for which it is used. Periodic reviews of requirements should be completed to reflect changing need. For examples, reviewing of the basket of indicators used to report corporate performance.

- **Complete** - All data should be collected in accordance with established definitions and procedures. Missing, incomplete, or invalid records will be monitored to provide an indication of data quality and can highlight issues for further investigation and improvement.

4. Who needs to read this policy?

4.1 This policy is to be used by officers who collect, analyse, and report any data which is used to support decision making. The document should also guide our partners who regularly submit and/or receive data and information to/from the council to support joint service delivery.

5. Scope

5.1 This policy applies to any information, whether written or numerical, held or produced in:

- Systems owned and managed by the council, e.g., where services are provided directly by the council

- Systems co-owned by the council but managed by a third-party, e.g., where services are delivered on the council's behalf through a shared services agreement.

- Systems owned and managed by partner organisations, e.g., where data is supplied to the council as the lead authority responsible within a partnership setting.

6. Systems and Responsibilities

6.1 The council will ensure that appropriate systems are in place for the collection, recording, analysis and reporting of data. It recognises the importance of these systems operating on a right first-time principle, as well as the principle of 'collect once and use numerous times' (COUNT) which will underpin data collection and storage.

6.2 When developing or implementing new information systems, the council will effectively consult with staff and partners.

6.3 To ensure data quality is managed effectively and to secure a culture of data quality throughout the council, responsibilities have been assigned as outlined below:

Chief Data Officer	The person designated with the organisational lead for ensuring that data is used to its maximum potential and data is of sufficient quality to provide insight to support effective decision making
Directors	Have overall responsibility for the quality of data within their service groupings and for ensuring the principles of data quality are met
Heads of Service and Strategic Managers	Have responsibility for data quality and driving improvement within individual teams. a. ensuring adequate, safe systems are in place to ensure adequate data quality This includes data definitions, documented procedures for collection and validation checks; b. ensuring data is accurate, timely and meets relevant local and national guidance; c. raising awareness of the data quality policy and ensuring staff responsible for data are aware of its requirements.
Strategy Team	Responsible for: a. regularly reviewing and reporting on compliance with the data quality policy and procedures and liaising with the appropriate officers to rectify any non-compliance; b. establishing and seeking agreement of a set of indicators to report on corporate performance; c. collation and promoting a manual of definitions; providing support and advice to services and developing the performance management framework to incorporate data

	quality; promoting the importance of data quality throughout the council and with partners; d. Reporting corporate performance quarterly including reporting of any data quality issues.
Service Teams	Designated officers with specific responsibility for collecting and reporting data within their service grouping. They will have responsibility for: a. co-ordinating definitions with data provider and ensuring systems are in place to collect and report data; b. ensuring that all data collection processes are documented and that there is an appropriate deputy responsible officer in place who understands the process and can maintain the day-to-day aspects of data collection; c. undertaking review of data accuracy for any reported performance data prior to submission; d. establishing systems to validate data quality and reporting back to those who provide data; informing Strategy Teams of any data that are restated or changes to data and/or supporting definitions as they arise. e. Carrying out validation checks for all performance indicators that are reported quarterly.
Systems Teams / Data Providers	Designated officers with specific responsibility for management of data and/or systems within their service grouping. Responsible for: a. the administration of the data system and ensuring that the data in the system is accurate. It is the responsibility of all staff who input, store, retrieve or otherwise manage data to ensure that it is of the highest quality; b. liaising with service performance teams in development and ownership of definitions. c. data quality and access control to data analytics for their allocated service area as part of a data stewardship role
Internal Audit	Responsible for: a. providing assurance on the effectiveness of the overall framework for data quality; b. providing advice and guidance on establishing data quality controls for new system developments and providing assurance on the effectiveness of data quality controls in existing systems; c. independently checking data linked to the internal audit review programme to provide assurance that it is accurate. d. Making recommendations for improvement in data quality e. Providing assurance to the Audit Committee
Data Protection Officer/ Info. Mgmt. Team	Monitoring compliance with the UK GDPR and other data protection laws, data protection policies, awareness raising and training.

Caldicott Guardian	Ensuring that personal information about those who use health and social care services is used legally, ethically, and appropriately and that confidentiality is maintained.
All council staff and members	Required to adhere to the Data Quality Policy, ensuring data is handled in a responsible way and all reasonable efforts are made to ensure the quality of data. Training and development of staff and an understanding of the importance of data quality for elected members will underpin the achievement of high levels of data quality. Staff will be supported in their responsibility towards capturing quality data. Data sharing issues with partners will be addressed by staff working closely with partners to resolve them. This includes taking reasonable steps in keeping personal data accurate and up to date in line with requirements of the GDPR. The commitment to data quality will be clearly communicated throughout the council to re-enforce the message. Policies, procedures and guidance will be developed and updated in association with relevant staff. To ensure this policy is embedded, key actions will be developed, monitored and reviewed

7. Partnership Working

7.1 Information sharing is crucial to effective partnership working. To ensure we have confidence in shared data or data supplied by third parties, we utilise a formal framework for data sharing with partners (e.g., data sharing protocols, clauses in procurement contracts). This includes identifying and complying with all relevant legal, compliance and confidentiality standards.

7.2 The council is committed to collecting and processing data in line with national (if available) or locally established standards. A set of quality requirements will be implemented to ensure that all data used by the council, shared externally, or provided by third-party organisations is of high quality.

8. Data security

8.1 The council will ensure that all business-critical systems have a secure environment and appropriate backup systems. Access to and use of data will be compliant with relevant legislation. Our processes will be regularly tested to ensure security and maintain robustness. In the event of any system failure or disaster, we have developed and will maintain adequate business continuity plans. These measures ensure that our data remains secure, available, and accurate, and our services can continue to operate effectively, even during unforeseen circumstances.

9. Data use and Reporting

9.1 The council will ensure that data is used appropriately and in the right forum, so reliable data is always at the centre of decision making. Reported information is

made available to staff who produce it to reinforce understanding of the way it is used.

10. Monitoring and Reviewing Data Quality

10.1 The council has a framework in place for monitoring and reviewing data quality, as well as addressing the results of data quality reviews. This ensures that risk associated with data quality is appropriately managed.

10.2 All services have in place specific arrangements for dealing with data quality concerns, such as incorrectly recorded personal information, delays completing and submitting statutory returns, or missing information which prevents a process or action. In the first instance, the concern is raised with a relevant manager. This should be escalated to the relevant manager. Data protection concerns should be dealt with in accordance with the council's Data Protection Policy.

10.3 The council will also formally report on data quality. Services report issues arising from data quality reviews through departmental management teams or managers, and the outcomes of internal audit reviews are shared with relevant officer groups and regularly reported to Audit Committee (enabling previously agreed improvement actions to be monitored to ensure they have been implemented).

11. References

- Data Quality Toolkit (Durham County Council)
- Data Quality – How to manage your data effectively - Staff Guide (Durham County Council)
- Data protection (think privacy) – Durham County Council

11.1 For advice regarding the application of this policy please contact: Performance@durham.gov.uk

Appendix A: Regulatory Framework for Data

This policy considers and follows the most recent government legislation and guidance, the governance of information has several legislative and guidance areas as follows:

- **Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).** Personal Information must be handled and stored in a confidential manner, in line with the Data Protection Principles.

- **Regulation of Investigatory Powers Act 2000**. Councils can collect and use information from a covert or human intelligence service for the purpose of investigating crime which may be subject to disclosure.

- **Freedom of Information Act 2000**. Public Authorities, if requested, must disclose information that they hold.

- **Environmental Information Regulations 2004**. Public Authorities, if requested, must disclose environmental information that they hold

- **Local Government Transparency Code.** All Local Authorities must publish the datasets required by the code, in some cases in prescribed format

- **Re-use of Public Sector Information regulations**. Encourages the re-use of public sector information by third parties for purpose no other than the initial public task it was produced for. Governs what and how information must be made available for re-use

- **Caldicott Principles**. Caldicott principles and processes provide a framework of quality standards for the management of confidentiality and access to personal information in relation to health and social care services under the leadership of a Caldicott Guardian