

Data Quality Standards

1.0 Introduction

Data quality is the ability to supply data that is fit for purpose and use in planning, operations and decision-making. Gloucestershire County Council uses data at all levels of the organisation and in a range of ways to support the delivery, oversight and design of services to members of the public and internally. Good data quality:

- Is crucial to operational and transactional processes and the reliability of business analytics and business intelligence reporting;
- Ensures that decision-making is based upon accurate, complete and adequate data, informing subsequent actions and effective service delivery;
- Protects Gloucestershire residents and council staff as they receive and deliver services;
- Has reputational and transparency value in maintaining stakeholders' trust in the council.

It is essential that the council has processes in place to record, capture, process, store, manage and dispose of data accurately and appropriately to ensure data quality, understanding that the level of detail required of data will depend on the purpose for which the data is being held. These standards represent the council's commitment to maintaining good data quality and sets out its approach to meeting this commitment.

These standards have been developed taking into account the council's responsibilities under the following legislation:

- General Data Protection Regulations (GDPR) 2016
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 1998

In addition, there are many information requirements specified in legislation governing the provision of services to children, adults, and other council services.

The standards also align with those developed by Integrated Care Boards (ICBs) so that the council has a consistent, matching approach to data quality with the NHS. These standards link with the council's strategic approach to digital working, as

explained in the corporate [2018-2023 Digital Strategy](#). It also supports the [Information & Data Management Strategy: 2019-2024](#).

2.0 Responsibilities

- **Staff** - All staff are responsible for demonstrating a commitment to good data quality; applying these standards when capturing and processing data including the archiving or destruction of data;
- **Commissioners and Contract Managers** – are responsible for ensuring that appropriate data quality requirements are built into contracts and specifications and regularly monitor providers' compliance with these requirements;
- **Commissioned Providers** - are responsible for applying these standards when capturing, processing and storing data on behalf of the council;
- **Information Asset Owners** – are responsible for ensuring there are appropriate controls and data quality measures in place for their assets and are accountable for the data quality within that asset, identifying issues of data lag and data quality;
- **ICT** – are responsible for providing and maintaining the technical architecture required to enable good data quality across the council; supporting staff to use the tools and assets within this architecture;
- **Performance and Improvement Manager and team** – are responsible for monitoring performance across the council and with colleagues, highlighting issues of data quality where these are evident in reported performance information and supporting the provision of an accurate and reflective picture of performance;
- **Data, Analysis and Insight Team** – is responsible for working with colleagues across the council to ensure that robust, consistent data are recorded within systems and available for reporting.

Further related roles and responsibilities are described in the [Information & Data Management Strategy](#).

The council also receives datasets from a number of sources that may not have met these standards when capturing data. GCC will need to work within the limitations of the dataset but where possible, will follow the actions below to ensure that data is robust.

3.0 Standards & Quality Characteristics

3.1 Accuracy:

- Data must be sufficiently accurate for its intended purposes, representing clearly and in appropriate detail the interaction provided at the point of activity.

- Accuracy is most likely to be secured if data is captured as close to the point of activity as possible (e.g. if the person who captures the data also enters it on the system; if data is entered onto a system as soon as it is captured).
- Datasets must be internally consistent (i.e. similar items should be recorded in the same format, appear in the same field, etc.).
- Reported information must provide a reflective picture of performance and should enable informed decision-making.
- Data sources, methods of calculation, dates and periods covered etc. must be made explicit, particularly where data or analysis is being published for self-service.
- Where data is provisional it must be clearly marked as such (preferably indicating when final data will be available).
- Where compromises have to be made on accuracy (for example, when based on a sample), the resulting limitations of the data must be made clear to its users.

3.2 Validity:

- The purposes for processing data, i.e. the legal basis, must be stated at the outset of the processing activity.
- Data must be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions.
- When used to analyse trends, data must be consistent between periods. Any change must be justified and the usefulness of doing so must outweigh the disadvantages of losing trends.
- When used for benchmarking, data must be consistent between organisations/departments.
- Wherever appropriate and when indicators comply with the relevant definitions, data must use relevant reference numbers/labels. Where proxy data is being used, it must be given a new reference number to avoid confusion.
- Where proxy data is used to compensate for an absence of actual data, this must be made explicit and appropriate caveats provided.
- All measures or indicators must have a clear owner, who is responsible for confirming validity of that data. In the absence of a data owner, whoever is producing or publishing the data must assume responsibility for ensuring its validity.
- Wherever possible, data verification and validation techniques must be used to cleanse data records.

3.3 Reliability:

- Data collection processes must be backed by clear, robust rationale and insofar as is possible, should remain consistent and stable across collection

points and over time, whether using manual or computer-based systems or a combination.

- Wherever possible, changes in definition must be avoided in order to be able to provide consistent trend data over time. Any changes must be justified and the usefulness of these must outweigh the disadvantages of losing trends.
- Managers and stakeholders must be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or methods.
- Where data is required on a regular or routine basis, it must be held in an appropriate and stable environment and there should be clear, documented processes in place for its production.

3.4 Timeliness:

- Data must be captured as quickly as possible after the event or activity it records.
- Data must be available for the intended use within a reasonable time period.
- Data must be available quickly and frequently enough to support information needs, particularly in relation to risk and risk reduction/prevention and to influence the appropriate level of service or management decisions.

3.5 Relevance:

- Data captured must be relevant (and not excessive) to the purposes for which it is used.
- Data must be reviewed periodically to reflect changing needs or circumstances.
- Data that is no longer relevant or required must be destroyed, in accordance with the relevant retention schedule or legislative requirements.
- When interpreting data or using it to draw particular conclusions, staff undertaking analyses must be as explicit as possible about the basis of their analysis, transparent about the data on which that analysis is based, and open to constructive challenge. If approved Generative AI tools are used to analyse data, this must be clearly identified and disclosed in line with the council's [Generative AI Policy](#).

3.6 Completeness:

- There must be consistent processes for collecting and capturing data.
- Missing or invalid fields can provide an indication of data quality and can also point to problems in the recording of certain data items.
- Staff must ensure that Information Asset Owners are notified of significant gaps in datasets in order that these gaps can be addressed.

3.7 Availability:

- Data must be as easily accessible as possible to those that need it in order to perform their duties.
- Insofar as is consistent with Data Protection and commercial interest considerations, data must be regarded as an organisational asset and should be stored and managed in a way that allows it to be used by the wider organisation. This is regardless of whether the data is held by council teams or providers commissioned to deliver services on the council's behalf.
- We will work towards promoting open access to data, insofar as this is consistent with protecting individual service users and commercial interests, in order to promote healthy debate, invite constructive challenge, encourage collective understanding, develop intelligence and where required, enable data portability.

3.8 Security:

- Appropriate, secure processes must be in place to ensure that data is retained only for as long as necessary, in line with business and legislative requirements. Processes will also be put in place to dispose of data securely and completely once the required retention period is complete and the data is no longer needed.
- There must be agreed processes in place to transfer data securely internally and externally between relevant individuals and bodies.
- Wherever possible, use pseudonymised data and when working with very small numbers, use appropriate suppression methodology.

3.9 Resource:

- All staff capturing, receiving, storing, archiving and deleting data must be adequately trained in how to carry out these processes appropriately, be aware of the importance of good data quality and their responsibility in implementing and maintaining it.
- The technical architecture, including systems and processes, needed to enable good data quality must be in place to cover immediate and long-term requirements.
- Contracts and specifications must be developed, agreed and monitored so that commissioned providers deliver good data quality as part of their services.
- Policies and procedures will be in place to support good data quality across the council.

3.10 Sharing and Handling:

- Insofar as is possible and appropriate, datasets should be joined, matched and linked across the organisation to support joined up working.

Commissioned providers should readily share data with the council so that performance, trends and data quality levels can be understood.

- Insofar as is possible and appropriate, data shared with partners can be used to facilitate effective partnership working.

4.0 Document Control

4.1 Document information

Owner:	Jenny Grodzicka, Head of Information Management Service (DPO)
Author:	Michelle Conway, IMS Team Manager (Records)
Reviewer:	Teresa Wilmshurst, IMS Team Manager (Records)
Board(s) consulted:	Information Board
Date created:	December 2019
Next review date:	June 2027
Approval:	Rob Ayliffe, Director – Policy, Performance & Governance
Date of approval:	23 July 2024
Scheme of Delegation ref:	DPPG1
Version:	2.0
Classification:	UNCLASSIFIED

4.2 Version History

Version	Version date	Summary of Changes
1.0	December 2019	First version
1.1	July 2021	Format changes, updated out of date links
1.2	January 2023	Accessibility review and updates to formatting. Broken links fixed.
1.3	March 2024	Broken links fixed
2.0	June 2024	Updated out of date links; added link to Generative AI Policy and new document information added.

4.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

4.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000