Cheltenham Borough Council
Data Quality Policy

Version control

Document name: Data Quality Policy

Version: 1.0

Responsible officer

- Claire Hughes, Corporate Director and Monitoring Officer

Approved by: Cabinet

Next review date: May 2026

Retention period: Delete one year after new version

Revision history

Revision date	Version	Description
May 2023	1	New Policy

Consultees

Internal

- Corporate Governance Group and Leadership Team

External

- N/A

Distribution

All Staff and Council Website

Contents

1. Introduction

1.1. Cheltenham Borough Council (the Council) is committed to high standards of data quality. Every care will be taken to ensure that the data and information used to support decision making is accurate, valid, reliable, timely, relevant and complete in line with the this Policy.

1.2. The Council recognises the importance that reliable information has on its ability to deliver and manage services, inform users and improve performance. Good quality, accurate and timely data is essential in the provision of reliable performance and financial information to support decision making at all levels. This Policy therefore provides an overarching, corporate approach to the management of data quality to support decision-making and compliance with the Data Protection Legislation[1]

1.3. This Policy is one of a suite of Council policies that have been implemented to ensure that the Council's data is not only of high quality but is maintained securely and is protected from external corruption. This Policy is supported by the following:

- Corporate Risk Register; Data Protection Policy;
- Email & Internet Use Policy;
- Information Security Policy;
- Gloucestershire Information Sharing Agreement;
- Risk Management Strategy;
- Data Protection and Security Incident Reporting Policy;
- CCTV Policy

1.4. This policy applies to managing the quality of data provided from systems:

(a) owned and managed by the Council e.g. where services are provided directly by the Council;
(b) co-owned by the Council and managed by a third party delivering services on behalf of the Council e.g. a shared services' arrangements.

2. Purpose and Scope

2.1. The purpose of this policy is to have in place arrangements for managing the quality of the data collected and used by the Council and sets out the Council's approach to ensuring that:

[1] means the UK GDPR derived from the General Data Protection Regulation (EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time and any successor legislation to the UK GDPR or the Data Protection Act 2018 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner

(a) information is of high quality, accurate, valid, reliable, timely, relevant and complete;
(b) data quality is fully embedded across all services and is a key consideration in collecting, processing or using data to support decision-making.

2.2. Given the variety of data held by the Council, and the impact on service users in maintaining accurate and transparent records, maintaining high levels of data quality is vital. The consequences of poor data quality for the Council can be very serious. Poor data can:

- undermine accountability and damage public trust;
- weaken frontline service delivery;
- lead to financial loss and poor value for money;
- leave the vulnerable at risk;
- undermine partnership working.

2.3. By achieving high standards of data quality, the Council will:

(a) have assurance in the information supplied so that there will be confidence in the decision making processes and strength in the relationship between it and its customers, partners and other stakeholders;
(b) provide and publish data which is reliable, timely and robust;
(c) be able to respond effectively to service provision and quality of life issues affecting its communities.

2.4. Data is commonly defined as “Groups of information that represent the qualitative or quantitative attributes of a variable or set of variables.”

2.5. This policy supports any data collection which in practical terms, means information held or produced by the Council, whether it is written or numerical and includes information about people, businesses, properties and specific Council operations such as the Customer Contact Centre, number of bins collected etc.

2.6. Data and information is also increasingly used by the local community. The public place reliance on the information that the Council provides. It is therefore important that any information or data that is provided to residents, is of the highest quality.

2.7. Data is used by external bodies, especially those who carry out inspections or audits of the Council. Data will be used in preparation for external assessments and it is therefore essential that any data the Council produces is of the highest quality and is ultimately accurate.

3. What makes good quality data?

3.1. Producing robust data is an integral part of the Council's operational, performance management and governance arrangements.

3.2. The following are the six key characteristics/principles of good quality data

(a) **Accurate** – Data should be sufficiently accurate for its intended purposes. Accuracy is most likely to be achieved if data is captured as close to the point of activity as possible. Data should be captured once only, although it may have multiple uses. The importance of the uses for the data must be balanced with the costs and effort of collection. Where compromises have to be made on accuracy, the resulting limitations of the data should be clear.

(b) **Valid** - Data should be recorded in an agreed format and used in compliance with recognised Council and national standards. Where proxy data is used to compensate for an absence of actual data, consideration should be given to how well this data is able to satisfy the intended purpose.

(c) **Reliable** - Data should reflect stable and consistent data collection processes across the Council. This will ensure progress made is 'real' rather than due to changes in calculation methods.

(d) **Timely** - Data should be available within a reasonable time period, quickly and frequently enough to support information needs. This ensures informed decisions can be made based on up-to-date information rather than data that is out of date and potentially of less value.

(e) **Relevant -** Data captured should be relevant to the purposes for which it is used. This entails periodic reviews of requirements to reflect changing needs.

(f) **Complete -** All data captured should be based on the information needs of the Council and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

3.3. The principles of data quality are not limited to corporate performance statistics but cover other types of information held by the Council, such as details of individuals, businesses etc. It is important that any issues relating to the quality of data are treated seriously and promptly.

3.4. Data quality concerns may include:

- incorrect recording of personal information;
- delays completing and submitting statutory returns; and
- missing information relating to the ability to process or action further areas of work.

3.5. Departments must have in place, specific arrangements for dealing with data quality concerns. Any concerns regarding the quality of data should be raised, in the first instance, with a relevant manager. Depending on the severity of the data quality issue, this may be escalated to the relevant Director and/or the Data Protection Officer.

4. Data quality objectives

4.1. The Council's corporate objectives for data quality define a framework of management arrangements which will assure its customers, partners and other stakeholders that the quality of its data is reliable and sustainable:

(a) to ensure that arrangements for governance, monitoring and review of data are formalised and an organisational culture that values the quality and reliability of data is fostered;
(b) to provide a framework of systems, policies and procedures to improve management of data within the Council and in partnership with others to ensure the highest possible data quality whilst ensuring that resources put into ensuring data quality are proportionate to the benefit gained;
(c) to provide effective training for staff on expectations in terms of the standards of data quality;
(d) to ensure that the information processed and used is held securely and confidentially in accordance with the Data Protection Act 2018, Freedom of Information Act 2000 and other applicable laws;
(e) to ensure that published information is accessible, timely, valid and accurate.

5. Data quality standards

5.1. The Council is committed to collecting and processing data according to national, or where these are not available, locally defined standards. A formal set of quality requirements will be applied to all data that is used by the Council, shared externally, or provided by a third-party organisation.

6. Systems and processes

6.1. The Council will ensure that appropriate systems are in place for the collection, recording, analysis and reporting of data. The Council will use the principle of 'collect once and use numerous times' (COUNT) to underpin data collection and storage. See the Annex to this Policy for 'Tips to help you improve the accuracy in data entry'.

7. Data Security

7.1. The Council will ensure that data is stored in a secure environment with appropriate security and system backups for all business critical systems. The access and use of data should be appropriate to the data user and comply with relevant legislation (such as the Data Protection Act 2018). Systems will be

regularly tested to ensure processes are secure. Adequate business continuity plans will be developed and maintained.

7.2. Data erasure is a large part of the UK GDPR. It is one of the seven data protection principles: Article 5(e) states that personal data can be stored for “no longer than is necessary for the purposes for which the personal data are processed.” Data erasure is also one of the personal rights protected by the UK GDPR in Article 17, the famous “right to be forgotten.” “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.” There are some exceptions to this latter requirement, such as the public interest. But generally speaking, the Council has an obligation to erase personal data it no longer needs.

7.3. Email data erasure can be quite simple and often it can be automated. The Council will apply an expiring email option that allows users to set messages for deletion after a designated length of time.

7.4. Links and attachments from unknown email accounts should never be clicked or downloaded. Once an attacker gains access to one account or device, it’s often easy to access others, meaning a mistake by one employee could compromise vast amounts of Council data.

8. Partnership Working

8.1. Information sharing is crucial to partnership working. It is essential that the Council has confidence in shared data or data supplied by third parties. The Council will ensure that a formal framework for data sharing with partners is put in place. This includes identifying and complying with all relevant legal, compliance and confidentiality standards. A validation process will be established for all data provided by partners or other third parties.

9. Data use and reporting

9.1. The Council will ensure that data is used appropriately and in the right forum, so that reliable data is at the centre of decision making. Arrangements will be put in place to ensure that data is also used to manage and improve the delivery of services. Reported information will be made available to staff who produce it to reinforce understanding of the way it is used.

10. Internal control and validation

10.1. The Council will ensure that it has effective validation procedures in place to ensure the accuracy of data used. Data returns will be supported by a clear and complete audit trail and subject to service, corporate and internal audit verification checks. Any errors discovered during the audit will be corrected within established

timescales and any improvement actions will be acted upon in order to continuously improve the Council's approach to data quality.

11. Responsibilities

11.1. To ensure that data quality is managed effectively and to secure a culture of data quality throughout the Council, it is important to provide a clear assignment of responsibility throughout the Council:

Directors	Have overall responsibility for the quality of data within their directorates and for ensuring the six principles of data quality are met (see section 3.2 of this Policy).
Managers	Responsible for: • the administration of their department/service's data system and ensuring that the data in the system is accurate; • data quality and driving improvements within their departments/services including raising awareness of this Policy and ensuring that all staff understand their own area of responsibility in relation to data quality; • ensuring that adequate, safe systems are in place, which hold an acceptable standard of information; • ensuring that the performance information they provide is accurate, timely and meets relevant guidance; • regularly reviewing and reporting on compliance with this Policy and liaising with the appropriate officers to rectify any non-compliance; • ensuring that all data collection processes are documented; • ensuring that the day to day aspects of data collection are maintained; • undertaking reviews of data accuracy for any medium and high risk data prior to submission; • monitoring the quality of data shared under the Gloucestershire Information Sharing Agreement; • managing the risks associated with data quality; • Compiling returns for the 'single data set' (see section 12 of this Policy).
Senior Information Risk Officer	Responsible for ensuring this Policy is embedded within the Council and that key actions are developed and regularly monitored and reviewed
Data Protection Officer	Responsible for monitoring compliance with the Data Protection Legislation
Internal Audit	Responsible for • Providing assurance on the effectiveness of the overall framework for data quality;

	• 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; Independently test checking data linked to the internal audit review programme to provide assurance on accuracy
All Council staff	Responsible for: • adhering to this Policy; • ensuring that data is handled in a responsible way; • making all reasonable efforts to ensure the quality of data; • inputting, storing, retrieving or otherwise managing data to ensure that it is of the highest quality; keeping personal data accurate and up to date in line with requirements of the Data Protection Act 2018

12. Statutory data returns – the Single Data Set

12.1. The 'single data set' comprises a list of all the data that the Government expects local authorities to produce and submit to it in any given year. In general terms, the 'single data set' was established to support the delivery of local statutory services and enable the Government to apply evidence-based decision making in local government. The 'single data set' is a catalogue of all data returns for local authorities and is not a list of target based performance measures.

12.2. Managers are responsible for compiling data for the returns that apply to the Council, ensuring they are accurate and produced on a timely basis.

13. Third party data quality

13.1. Data quality is a key element in partnership working. It is important that, when establishing any new partnership, data quality forms an integral part to the partnership's governance arrangements.

13.2. Departments that rely on data from third party sources must ensure that they have mechanisms by which they are able to check the data for accuracy so that reliance can be placed on the data being received.

14. Data Sharing

14.1. Sharing of information is crucial to the successful delivery of local services. The Council is a signatory to the Gloucestershire Information Sharing Agreement (GISPA).

14.2. The GISPA provides for openness and transparency in information sharing, as well as appropriate governance and support, in order to assist signatory organisations and public bodies to share personal information lawfully, safely and securely.

14.3. Data shared under the GISPA must be of high quality i.e. meet the six principles of data quality (see section 3 of this Policy).

15. Performance data

15.1. Agreed performance targets will be entered onto the Clearview system, with any supporting information needed to verify the data. The data will be reported to Management Team on a monthly basis and on a quarterly basis, to Cabinet and the Overview and Scrutiny Committee.