Policy: Data Quality Policy

Author: Information Governance Team

Date: May 2021

Version: V1.0

GMCA GREATER MANCHESTER COMBINED AUTHORITY

GMCA, Churchgate House, 56 Oxford Street, Manchester, M1 6EU

Document Version Control

Document Type:	**Ref number**:
Document Name:	**Classification**:
Requirement for Document:	**Target Audience:**
Executive Summary:	
Executive Lead:	**Document Author:**
Ratified by/Approving Committee:	**Date Ratified**:
Date issued:	**Review Date:**
Circulation:	
Consultation:	
Superseded Documents:	**Cross Reference – Related policies and procedures:**
Date of Equality Impact Assessment:	**Date of DPIA:**
Contact Details for further information:	

Document Version

Version Date	Type of Change	Date	Revisions from previous issues	By

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

1.1. The Greater Manchester Combined Authority (GMCA) makes effective and wide-ranging use of information to realise the vision is to make Greater Manchester one of the best places in the world to grow up, get on and grow old. The Greater Manchester Strategy sets out a set of clear priorities for delivering this goal,

1.2. The GMCA recognises that reliable high quality information is essential and the availability of complete, accurate, relevant, accessible and timely data is fundamental in order to achieve its goals.

1.3. High quality performance information allows the GMCA to:

- understand how we are progressing against our priorities
- ensure that service delivery is effective
- make the right decisions and at the right time;
- inform our strategies and ensure we focus our resources where they are most needed;
- empower local people and account for our performance.

1.4. All decisions, whether service delivery, performance management, managerial or financial need be based on information which is of the highest quality.

1.5. This policy document underpins the GMCA's objective to record and present information of the highest quality and sets out high level principles as to how this will be achieved. It outlines who this policy applies to and the principles that staff must be aware of and adhere to. It also defines the governance arrangements, the key roles and provides protocols to ensure robust data quality is embedded throughout the GMCA assets.

2. Scope

2.1. This policy applies to all data including personal and special category/criminal conviction data used, stored or shared by or with the GMCA whether in paper or digital form and wherever it is located. It also applies to all data processed by the GMCA on behalf of other organisations.

2.2. The policy covers all data that is entered onto computerised systems within the GMCA and all paper-based records. It covers primarily data relating to research, the delivery of services, financial management, service management, performance management, corporate governance and communications. However, it should be noted that this policy is not restricted to just performance indicators.

2.3. It is intended to cover the collection, recording, validation, further processing and reporting of all types of information generated and used within, or reported externally, by the GMCA.

2.4. This policy applies to all GMCA employees, seconded staff members, volunteers, third party contractors, temporary staff and employees of other organisations who directly or indirectly support GMCA services.

3. Policy Statement

3.1. As the GMCA generates a wide range of information for a whole variety of uses, this policy statement does not provide detailed guidance for specific data items or individual areas of application; these are contained within the supporting protocols and procedures.

3.2. It concentrates instead on general principles of completeness, accuracy, ongoing validity, timeliness, consistency of definitions and compatibility of data items and signposts where specific procedures guidelines need to exist.

4. Roles and Responsibilities

4.1. **Chief Executive**

The Chief Executive is ultimately responsible for the organisation's compliance with data protection legislation. Part 7 of the DPA 2018 stipulates the CEX's liability with regards to offences committed under the Act.

The Chief Executive is ultimately responsible for ensuring the quality of GMCA's data and information.

4.2. **Monitoring Officer**

The Monitoring Officer is responsible for ensuring the lawfulness and fairness of GMCA decision making and must report on matters they believe are, or are likely to be, illegal or amount to maladministration. They are also responsible for matters relating to the conduct of members and officers.

The GMCA Solicitor is the Monitoring Officer.

4.3. **Senior Information Risk Owner (SIRO)**

The SIRO has an overall strategic responsibility for governance in relation to data Protection risks and is responsible for:

- Acting as an advocate for managing information risk within the GMCA
- championing and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers.

- Owning the organisation's overall information risk policy and risk assessment processes which encompasses Data Quality and Records Management and ensuring they are implemented consistently by IAOs
- Providing written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk.
- Owning the organisation's information incident management framework.

The SIRO for the GMCA is the Treasurer.

4.4. **Data Protection Officer (DPO)**

Under the Data Protection Legislation all public authorities must appoint a DPO. The DPO is responsible for:

- Informing and advising the GMCA and its employees of their data protection obligations. Monitoring compliance with the Data Protection legislation and internal data protection policies and procedures.
- Monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advising on whether a DPIA (data protection impact assessment) is necessary, how to conduct one and expected outcomes.
- Acting as the contact point for the supervisory authority (Information Commissioners Office) on all data protection issues, including data breach reporting.
- Serving as the contact point for data subjects e.g. employees, customers on privacy matters, including DSARs (data subject access requests).

The GMCA will meets its obligations regarding the DPO role and as such will ensure that:

- the DPO is involved, closely and in a timely manner, in all data protection matters;
- the DPO reports to the highest management level of your organisation, i.e. board level at the GMCA this is the SIRO;
- the DPO operates independently and is not dismissed or penalised for performing their tasks;
- adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) is provided to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge;
- the DPO has the appropriate access to personal data and processing activities;
- appropriate access to other services within your organisation so that they can receive essential support, input or information.

The Data Protection Officer for the GMCA is the Assistant Director of Information Governance.

4.5. **Information Asset Owners (IAOs)**

Information Asset Owners (IAOs) role is to understand in their business area what information is held, what is added and what is removed, how information is moved, and who has access and why.

The IAO is responsible for:

- ensuring they are understand and address risks to the information.
- ensure that information is fully used within the law for the public good.

- providing a written judgement of the security and use of their asset annually to support the audit process.
- Ensuring that the data they are responsible for is complete, accurate, relevant, accessible and timely

4.6. **Information Asset Administrators (IAA)**

An IAO is accountable for the information assets under their control but may delegate day to day management responsibility to an IAA who would be responsible for:

- Managing the joiners, movers and leavers process within the team which may cut across the organisation and partner boundaries.
- Ensuring all team members keep their training up-to-date
- Managing the day to day security of the asset including access control management
- Identifying potential or actual security incidents and consulting the IAO on incident management ensuring that risk assessments and other documents for projects are accurate and maintained
- Keeping and regularly reviewing records of Processing Activity
- Management of Information Asset Register (IAR)
- Act as gatekeeper ensuring that the Information Asset Owner is aware of any changes to the information asset or its use.
- Assist the IAO in ensuring that data is complete, accurate, relevant, accessible and timely

4.7. **Information Security Officer**

The Information Security Officer is responsible for developing and implementing the GMCA Information Security and associated policies and procedures to reflect local and national standards and guidance and legislative requirements. They also support the GMCA in ensuring compliance with information security requirements. This role reports to the Deputy Chief Information Officer.

4.8. **Heads of Department will;**

- Ensure all managers are made aware of this policy and understand their duties to ensure compliance across their teams.
- Notify the Information Governance Team and seek advice where activities involve the use of personal data. This includes any new projects, new data processing or any changes to existing processing
- Ensure compliance with GDPR and Data Protection Legislation for all teams within their area.
- Ensure all employees are appropriately trained in the safe handling and use of information and as a minimum complete the GMCA's data protection training every year.
- Ensure that the data they are responsible for is complete, accurate, relevant, accessible and timely

4.9. **Line Managers will;**

- Ensure that their teams are made aware of this policy and understand its requirements.
- Fully implement the requirements of this policy within their teams.

- Ensure all employees are appropriately trained in the safe handling and use of information and as a minimum GMCA's data protection training every year.
- Ensure that the data they are responsible for is complete, accurate, relevant, accessible and timely

4.10. **All staff must;**

- Follow this policy when processing of data throughout the GMCA.
- Protect any data or information within their care.
- Seek additional advice and guidance from their manager, Information Governance Team or the Data Protection Officer if unsure or in any doubt about how to handle information.
- Report any suspected or actual data breaches or any breaches of this policy to their line manager or the Information Governance team as soon as they become aware in line with the Serious Information Governance Incident procedure.
- Keep up to date with all GMCA Data Protection and Information Governance training that is appropriate to their role
- Ensure that the data they are responsible for is complete, accurate, relevant, accessible and timely

4.11. **Information Governance team will;**

- Will be the source of subject matter expertise in relation to data protection
- Develop and inform strategies in relation to the use of personal data
- Provide strategic oversight to large scale programmes of personal data sharing
- Will advise on and provide support in relation to data protection and the handling and use of personal data.
- Will provide guidance and support to staff undertaking Data Protection Impact Assessments.
- Develop and maintain relevant policies and procedures in line with changes to legislation and best practice.
- Manage and monitor requests from Data Subjects who choose to exercise their individual rights including Subject Access Requests in line with GMCA policies and procedures.
- Manage and monitor any Information Security Breaches in line with the GMCA Information Security Breach Policy.
- Develop and deliver training as required
- Will monitor compliance with this policy

5. The importance of good data quality

5.1. The General Data Protection Regulations 2018 principles state that personal data shall 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."

5.2. Data quality is one of the key elements of the GMCA's Information Governance Framework which sets out the agreed approach for managing information as an asset. This applies to all information held by the organisation.

5.3. Information held by GMCA must be;

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically; and
- shared appropriately and legally

5.4. The availability of complete, accurate, relevant, accessible and timely data is important in supporting decision-making, planning, resource allocation, accountability, and the delivery of service outcomes and priorities; for example:

- Strategic / planning - High quality data and information is necessary to plan the GMCA's vision and goals, and inform the decisions that underpin everything the organisation does.
- Financial planning - data must be reliable to enable budget setting and forecasts to support service planning.
- Service planning - accurate data about the volume and type of services delivered and activities undertaken is essential to ensure appropriate allocation of resources and future service delivery.
- Performance management - accurate data enables the identification and resolution of poor performance against standards and targets.
- Service improvement - accurate data enables analysis of service provision to identify areas for improvement.
- Customer support - accurate data enables delivery of relevant and timely services.
- Efficient administration - Data provided to an appropriate standard and in such a way that the full range of stakeholders, partners and agencies can access the information they need easily and quickly.
- Audit processes - Data available for timely, reliable and accurate reporting to support internal and external audit regimes.
- Accountability, Transparency and Open Data Good quality data is essential in delivering the GMCA's transparency and open data agenda.
- Partnership Working - Information sharing is crucial to partnership working and facilitating effective public service reform.

5.5. The GMCA has identified seven key characteristics of good quality data:

1. **Accuracy -** Data should be sufficiently accurate for the intended use, not be misleading as to any matter of fact, and should be captured only once, although it may have multiple uses. Data should be captured at the point of activity. Data should be kept up to date and any inaccurate data, having regard to its purpose, should be erased or rectified without delay.
2. **Validity -** Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions. This will

ensure consistency between periods and with similar organisations, measuring what is intended to be measured.

3. **Reliability -** Data recorded should reflect stable and consistent data collection processes across collection points and over time. Progress toward performance targets should reflect real changes rather than variations in data collection approaches or methods. The mechanism for collecting and storing data should do so without contradiction or unwarranted variance.
4. **Timeliness -** Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence service or management decisions.
5. **Relevance -** Data captured should be relevant to the purposes for which it is to be used. This will require a periodic review of requirements to reflect changing needs. There should be a level of consistency between the data content and the purpose.
6. **Completeness -** Data requirements should be clearly specified based on the information needs of the organisation and data collection processes matched to these requirements.
7. **Accessibility –** Where there are no legal or regulatory constraints, individuals using data should have the right level of access in order to perform the task effectively.

6. Risk Management

6.1. The key risks associated with data quality problems are:

- Negative consequences, financial and other, as a result of submitting inaccurate or misleading data.
- Inappropriate decision-making and inefficient/ineffective provision of GMCA/GMFRS services
- Reputational damage.
- Harm to an individual or group of individuals where GMCA has a duty to protect
- Affecting relations and data sharing arrangements with partners and agencies.
- Regulatory action and fines from the Information Commissioner for breaches of DPA or FOI legislation.

6.2. There are three main high level aspects of risk management in respect of Data Quality; the identification of compliance requirements, the identification and assessment of business risks and the application of risk mitigation measures.

1. Identification of compliance requirements

Through the use of resources and ongoing assessment the GMCA is monitored and judged on the quality of the information it produces. This is especially important in terms of national indicators, local indicators (e.g. the business service plan) and other information reported to central government departments all of which depend on good quality data for their accuracy and supporting evidence.

Statutory, regulatory and other local compliance requirements will be reviewed and incorporated into the Data Quality Standard and supporting protocols as appropriate.

2. Identification and assessment of business risk

Ever-increasing use of computerised systems provides greater opportunities to store and access many types and large volumes of data, but also increases the risk of misinformation, and therefore poor decision-making, if the data from which information is derived is not good quality. This risk applies to the GMCA's internal use of information, to information received from Government and its various agencies and to data shared with external partners. For information to have value it is essential that the data is consistent, accurate and complies with all appropriate l standards

3. Application of risk mitigation measures

In order to mitigate the risks to the business and its information a number of measures will be put in place

A framework of protocols and guidance will be produced covering the following areas:

- Data Quality Standards
- Data Quality indicators
- Governance
- Roles and Responsibilities
- Training and awareness
- Correcting Data to ensure accuracy, completeness and validity
- Manipulation and Reporting
- Monitoring and evaluation
- Data Minimisation

6.3. It is for the above reasons that the GMCA requires a Data Quality Standard that will sit together with the Data Quality policy and supporting protocols.

7. Data Quality Requirements

7.1. In order to meet the characteristics of good data quality, the GMCA will ensure that it will adopt the following:

7.2. A principle of 'collect once and use numerous times' to underpin data collection and storage.

7.3. A formal set of quality requirements based on national and local standards to be applied to all data that is used by the Council, shared externally, or provided by a third-party organization.

7.4. **Accountability;**

Procedures, induction and training for all staff with responsibility for data processing that should cover;

- The need for good quality data and how staff contribute to it;

- Individual responsibilities with regard to data collection, storage, analysis and reporting;
- Awareness of the relevant legal and statutory requirements
- Data is stored, used and shared in accordance with the law, including those for data protection and freedom of information.
- Responsibility to report any systematic data quality issues immediately to a manager who should ensure remedial action is taken;
- Will erase personal data it no longer needs.

Policies and Procedures;

- Local procedures must exist for all key activities such as large scale data collection, analysis and reporting and be easily available to staff
- Policies and procedures must be easily available and reviewed regularly to consider their impact on data quality and to ensure they reflect any changes within the service areas
- Heads of service must ensure policies and procedures are adopted and embedded within local processes and that compliance is achieved

.

Systems and Security;

- Appropriate security arrangements to ensure that data is protected from unauthorized access;
- Security arrangements in place to ensure appropriate levels of access to data by individual staff including role based access controls
- Data Quality is a core component when specifying / procuring IT Systems.
- Appropriate systems are in place for the collection, recording, analysis and reporting of data

8. Compliance with data quality principles

8.1. Any breaches of the principles in this policy must be reported to the information governance team immediately; OfficeOfDPO@greatermanchester-ca.gov.uk.This includes an errors / incidents or breaches which have occurred.

8.2. Failure to comply with the Data Quality or associated Data Protection policies may result in disciplinary action in line with HR processes.

9. Policy exemption

9.1. Occasionally there may be situations where exceptions to this policy are required, as full adherence may not be practical, could delay business critical initiatives or could increase costs.

9.2. Where the significance and purpose of the data does not justify a particular aspect (for example the cost of building an internal system validation check

outweighs the benefit of the additional data accuracy) then this should be risk assessed on a case by case basis. Where there are justifiable reasons, the Data Protection Officer must be consulted immediately; OfficeOfDPO@greatermanchester-ca.gov.uk .

10. Review

10.1. This policy will be reviewed at least annually by the Information Governance Team to ensure that it is updated in line with any changes in legislation. It may be revised more frequently if necessary if there are any changes in legislation or national policy.

11. Training and Awareness

11.1. Staff will be made aware of this policy by it being hosted on the Information Governance section of the GMCA intranet.

11.2. The GMCA will provide relevant training both online and face to face to ensure that staff understand the legislation, the requirements of this policy and its application to their role.

11.3. All staff must complete mandatory data protection training every year and undertake any further training provided by the GMCA to enable them to perform their duties appropriately.

12. Compliance and Monitoring

12.1. The GMCA will continue to review this effectiveness of this policy to ensure that it is achieving it intended purpose

12.2. Completion of training will be monitored by the Information Governance Team and all employees must have regard to the Data Protection legislation and this policy when collecting, accessing, using, disclosing or destroying information.

12.3. Failure to follow this policy may result in disciplinary proceedings and/or legal prosecution.

12.4. If an employee is in any doubt about how to handle information including personal information, they should speak to their line manager or contact the Information Governance Team at OfficeofDPO@greatermanchester-ca.gov.uk.

13. Contact details

Phillipa Nazari Data Protection Officer; Assistant Director Information Governance

GMCA, Churchgate House, 10, Oxford Street, Manchester M1 6EU

Email: OfficeofDPO@greatermanchester-ca.gov.uk

Information Governance Team;

GMCA, Churchgate House, 10, Oxford Street, Manchester M1 6EU

Email; OfficeOfDPO@greatermanchester-ca.gov.uk

Appendix

Appendix 1 - Legislative Framework

The Data Quality Policy is set in the context of the following legislation and guidance:

- UK General Data Protection Regulation 2018 and Data Protection Act 2018 – that requires that personal information must be handled and stored in a confidential manner
- The Human Rights Act 2000 - everyone has the right to respect for their private and family life, home and correspondence.
- Freedom of Information Act 2000 and Environmental Information Regulations 2004 - Public authorities, if requested, must disclose information that they hold.
- Localism Act 2011 - Highlights the importance of transparency and accountability of public bodies and raw data.
- Local Government Transparency Code - All local authorities must publish the datasets required by the code, in some cases in prescribed formats
- The Re-use of Public Sector Information Regulations 2015 (PSI) Encourages the reuse of public sector information by third parties for purposes other than the initial public task it was produced for. Governs what and how information has to be made available for re-use.