Public Document

GMCA GREATER MANCHESTER COMBINED AUTHORITY

GREATER MANCHESTER COMBINED AUTHORITY
RESOURCES COMMITTEE

DATE: **Friday, 30th July, 2021**

TIME: **10.00 am**

VENUE: **Committee Rooms 2, 3 & 4, Trafford Town Hall, Talbot Road, Trafford, M32 0TH (Sat-nav post code M16 0QQ)**

AGENDA

1. Apologies

2. Appointment of Chair

To appoint a Chair to the GMCA Resources Committee for 2021/22

3. Membership of the Resources Committee 2021/22

To note the membership of the GMCA Resources Committee 2021/22 as agreed by the GMCA Annual Meeting on 25 June 2021, as follows:

Mayor of Greater Manchester, Andy Burnham (Lab)
David Greenhalgh (Bolton) (Con)
Richard Leese (Manchester) (Lab)
Elise Wilson (Stockport) (Lab)
Paul Dennett (Salford) (Lab)
Brenda Warrington (Tameside) (Lab)
David Molyneux (Wigan) (Lab)

4. Resources Committee Terms of Reference 1 - 4

To note the GMCA Resources Committee Terms of Reference.

5. GMCA Information Governance Policies 5 - 86

Report of Eamonn Boylan, Chief Executive Officer, GMCA &

BOLTON	**MANCHESTER**	**ROCHDALE**	**STOCKPORT**	**TRAFFORD**
BURY	**OLDHAM**	**SALFORD**	**TAMESIDE**	**WIGAN**

Please note that this meeting will be livestreamed via www.greatermanchester-ca.gov.uk, please speak to a Governance Officer before the meeting should you not wish to consent to being included in this recording.

TfGM.

6. Core Investment Team - Transactional Posts 87 - 96

Report of Eamonn Boylan, Chief Executive Officer GMCA & TfGM.

For copies of papers and further information on this meeting please refer to the website www.greatermanchester-ca.gov.uk. Alternatively, contact the following Governance & Scrutiny Officer:
✉ sylvia.welsh@greatermanchester-ca.gov.uk

This agenda was issued on 22 July 2021 on behalf of Julie Connor, Secretary to the Greater Manchester Combined Authority, Broadhurst House, 56 Oxford Street, Manchester M1 6EU

RESOURCES COMMITTEE – TERMS OF REFERENCE

1. Purpose

1.1 To consider issues relating to the establishment and implementation of human resource processes and policies of the GMCA.

1.2 To oversee issues relating to the effective and efficient use of ICT and Property resources for the GMCA.

2. Composition

2.1 Membership

The Resources Committee will be appointed by the GMCA annually.

The Committee will comprise seven members of the GMCA.

2.2 Political Balance

In appointing members of the Resources Committee the GMCA will act in accordance with Rule 15.3 of the GMCA Procedure Rules set out in Section A of Part 5 of this Constitution.

2.3 Chairing the Committee

The GMCA shall appoint the Chair of the Committee. In the absence of the appointed Chair, the Committee will be chaired as determined by the Committee.

2.4 Quorum

The quorum for the Resources Committee shall be three.

2.5 Voting

Each member to have one vote, no member is to have a casting vote

3. Role and Function

3.1 The GMCA's Resources Committee has the following role and functions (except insofar as they are delegated to the Chief Fire Officer):

(a) To consider, approve and adopt any new, or significant revision to existing human resources strategies and policies insofar as they relate to the appointment, terms and conditions of employment and dismissal of staff.

(b) To determine any other matters relating to the appointment, terms and conditions of employment and dismissal of staff which are neither covered

by policies of the GMCA nor delegated to Officers under the GMCA's Scheme of Delegation.

(c) To make decisions in relation to the establishment and remuneration of new and additional posts whose remuneration is, or is proposed to be, in excess of Grade 11 or equivalent, but less than £100,000, per annum.

(d) To make recommendations to the GMCA in relation to the establishment and remuneration of new and additional posts whose remuneration is, or is proposed to be, £100,000 or more per annum.

(e) To make decisions in relation to severance packages above £60,000 but less than £95,000.

(f) To make recommendations to the GMCA in relation to severance packages of £95,000 or more.

(g) To determine the payment of honoraria exceeding 12 months duration in respects of posts in excess of Grade 11 or equivalent.

(h) To determine claims arising under the Scheme of Allowances for employees injured in the course of their employment above £10,000.

(i) To determine policies relating to pensions and discretionary compensation for early termination of employment.

(j) To constitute the Employers' side of any Local Joint Committee with the relevant trade unions.

(k) The consideration of and recommendation to the GMCA of the determination of collective terms and conditions of service and the annual pay policy statement.

(l) To consider the outcomes of staff engagement and consultation exercises, particularly issues raised by the Workforce Engagement Board.

(m) The making of agreements with other local authorities for the placing of staff at the disposal of those other local authorities.

(n) To establish at the appropriate time panels of members as a sub-committee to act as appointment panels for the appointment of the Head of Paid Service and Chief Officers of the GMCA.

(o) To consider major staffing and organisational reviews.

(p) To provide the Head of Paid Service, Monitoring Officer and Treasurer with such staff as are in their opinion sufficient to allow their statutory duties to be performed.

(q) To determine appeals against dismissal and to establish a Resources (Employee Appeals) Sub-Committee for this purpose.

(r) To oversee ICT and Property matters and make recommendations to the GMCA where appropriate.

(s) Oversight of the GMCA's Business Plan.

4. Delegation

4.1 In exercising the above powers and responsibilities, the Committee shall have delegated power to make decisions on behalf of the GMCA, except for any matter where:

(a) the Head of the Paid Service determines the matter should be considered by the GMCA; or

(b) the GMCA has resolved to determine the matter.

4.2 The Committee may itself determine not to exercise its delegated powers and instead make recommendations to the GMCA where it considers this is appropriate.

GMCA GREATER MANCHESTER COMBINED AUTHORITY

RESOURCES COMMITTEE

Date: 30 July 2021

Subject: GMCA Information Governance Policies

Report of: Eammon Boylan, Chief Executive

PURPOSE OF REPORT

The report presents a set of information governance policies for GMCA that will provide a clear framework for employees, ensuring that they understand their role in supporting the GMCA's organizational compliance.

RECOMMENDATION

The Committee is asked to approve the appended information governance policies:

- Appropriate Policy (Special Category Data)
- Data Subject Rights Policy
- Data Quality Policy
- Anonymization and Pseudonymization Policy
- Freedom of Information and Environmental Information Regulations Policy.

CONTACT OFFICERS:

Steve Wilson – GMCA Treasurer and Senior Information Risk Owner
steve.wilson@greatermanchester-ca.gov.uk

Phillipa Nazari – Assistant Director Information Governance and Data Protection Officer
phillipa.nazari@greatermanchester-ca.gov.uk

1.0 BACKGROUND

1.1 Data protection law specifically requires organisations to put in place effective data protection policies, to enable them to take the practical steps to comply with their legal obligations. The Data Protection Act came into force in thew UK in 2018. It outlines that employees can face prosecution for data protection breaches. As with previous legislation, the new law contains provisions making certain disclosure of personal data a criminal offence.

1.2 The following set of GMCA organizational policies are intended to provide clarity and consistency for employees, by communicating what people need to do and why, to help them avoid the potentially serious, criminal implications for employees that can arise from failure to comply with data protection legislation. Examples from the Data Protection Act (2018) include:

Section 148: Destroying or falsifying information and documents etc. (Data Quality). Under Section 148 (2) (a) it is an offence for a person to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material.

Section 173: Alteration etc. of personal data to prevent disclosure to data subject (Data Subject Requests).

Section 173 relates to the processing of requests for data from individuals for their personal data. Section 173 (3) makes it a criminal offence for organisations (persons listed in Section 173 (4)) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure.

Section 171: Re-identification of de-identified personal data (anonymization and pseudonymization)

Section 171 - a new offence - criminalizes the re-identification of personal data that has been 'de-identified' (de-identification being a process - such as redactions - to remove/conceal personal data). Section (5) states that it is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified.

1.3 In relation to the Freedom of Information Act (2000) Section 77 states a person "*is guilty of an offence if he alters, defaces, blocks, erases, destroys or conceals any record held by the public authority, with the intention of preventing the disclosure by that authority of all, or any part, of the information to the communication of which the applicant would have been entitled*."

1.4 The attached policies have been drafted by the GMCA Information Team in conjunction with the GMCA Information Governance (IG) Board. The Freedom of Information and Environmental Information Regulations Policy was considered and agreed with Trade Unions representatives in October 2020.

1.5 All policies follow an agreed format and style, including arrangements for document version control.

2.0 APPROPRIATE POLICY (SPECIAL CATEGORY DATA)

2.1 As part of the Greater Manchester Combined Authority's (GMCA) statutory and public functions, it processes special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

2.2 This policy applies when the GMCA is processing special category data when relying on the requirements listed in Parts 1, 2 and 3 of Schedule 1 of the Data Protection Act 2018. This policy lists the procedures, which are in place to secure compliance with the General Data Protection Regulation and data protection principles, needed when processing special category data. It applies to all GMCA staff. "Staff" for the purposes of this policy includes GMCA officers, including contractors, consultants and agency staff.

2.3 The Appropriate Policy (Special Category Data) is attached as appendix 1.

3.0 DATA SUBJECT RIGHTS POLICY

3.1 This policy provides an introduction to the rights individuals have under the data protection legislation.

3.2 The rights of individuals ('data subjects') in relation to the processing of their personal information are set out in the General Data Protection Regulation (GDPR). Further provisions relating to the data rights of individuals can be found within the Data Protection Act 2018 (DPA 2018), which include law enforcement activities and other areas not covered under the GDPR.

3.3 The GDPR strengthens these existing rights. The changes are mostly evolutionary but also give individual's rights in other areas such as the right to data portability. Some of these rights are subject to limitations and exceptions; further details of which may be viewed below.

3.4 The Data Subject Rights Policy is attached as appendix 2.

4.0 DATA QUALITY POLICY

4.1 The Greater Manchester Combined Authority (GMCA) recognizes that reliable information is essential and the availability of complete, accurate, relevant, accessible and timely data is fundamental in supporting the GMCA to achieve its goals. The GMCA recognizes that all decisions, whether service delivery, performance management, managerial or financial need be based on information which is of the highest quality.

4.2 The data quality 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.

4.3 The Data Quality Policy is attached as appendix 3.

5.0 ANONYMISATION AND PSEUDONYMISATION POLICY

5.1 Effective pseudonymization and/or anonymization processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality. They are part of the Data Protection by Design approach (Article 25 of GDPR) through which data protection is integrated into processing activities and business practices, from the design stage right through the lifecycle. They will often be relevant to a Data Protection Impact Assessment (DPIA) and form a key technical measure to ensure processing complies with the data protection principles (Article 35 of GDPR).

5.2 This policy therefore sets out how the GMCA will comply with the Data Protection legislation in order to ensure that the personal data it holds is used appropriately, processed safely and securely and that individuals are able to exercise their rights.

5.3 The Anonymization and Pseudonymization Policy is attached as appendix 4.

6.0 FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS POLICY

6.1 As an organization, one of the most frequent types of requests we receive are Freedom of Information requests. In order to support the organization in managing these requests, and in order to ensure that we are compliant to Data Protection Act 2018, General Data Protection Regulation and Freedom of Information Act 2000 we have produced new guidance which includes a policy, procedure, frequently asked questions and a guide to exemptions.

6.2 This policy sets out our organizational approach to Freedom of Information and Environmental Information Regulation requests. The policy has been approved by the Unions.

6.3 The Freedom of Information and Environmental Information Regulations Policy is attached as appendix 5.

7.0 NEXT STEPS

7.1 Subject to approval of the policies by this Committee, an updated training offer for employees will be delivered alongside a communications plan (both for all employees and key stakeholders) to ensure that employees are aware of and understand their obligations in relation to the respective policies.

8.0 RECOMMENDATION

8.1 The Resources Committee is asked to approve the appended GMCA information governance policies:

- Appendix 1 - Appropriate Policy (Special Category Data)
- Appendix 2 - Data Subject Rights Policy
- Appendix 3 - Data Quality Policy
- Appendix 4 - Anonymization and Pseudonymization Policy
- Appendix 5 - Freedom of Information and Environmental Information Regulations Policy

Policy: Appropriate Policy – Processing Special Categories of Data

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

Document Version Control 2
1. Introduction 4
2. Scope 4
4. Special category data 5
5. Criminal conviction data 5
6. Roles and Responsibilities 6
7. Conditions for processing special category and criminal offence data 9
7.2 Part 1 – Conditions relating to employment, social security and social protection 9
7.3 Part 2 – Substantial Public Interest Conditions 9
7.4 Part 3 – Additional Conditions Relating to Criminal Convictions, etc. 11
8. Procedures for ensuring compliance with the Principles 11
8.1 Accountability principle 11
8.2 Principle 1: Lawfulness, Fairness and Transparency 12
8.3 Principle 2: Purpose Limitation 12
8.4 Principle 3: Data Minimisation 13
8.5 Principle 4: Accuracy 13
8.6 Principle 5: Storage Limitation 13
8.7 Principle 6: Integrity and Confidentiality (security) 14
9. Review 15
10. Training and Awareness 15
11. Compliance and Monitoring 16
12. Data Protection Officer 16
13. General Enquires 16

1. Introduction

1.1 In order for Greater Manchester Combined Authority's (GMCA) to carry out its statutory and public functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

1.2 This policy applies when the GMCA is processing special category data when relying on the requirements listed in Parts 1, 2 and 3 of Schedule 1 of the Data Protection Act 2018. This policy sets out the safeguards, which are requiredto secure compliance with the General Data Protection Regulation and data protection principles, when processing special category data.

1.3 Under DPA 2018 Schedule 1, Part 4, there is a requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain conditions. This document fulfils that requirement and should be read together with the GMCA Data Protection Policy.

1.4 This policy explains our procedures and compliance with the data protection principles in Article 5 GDPR and our policies in relation to retention and erasure of this personal data.

1.5 In addition, it provides some further information about our processing of special category and criminal offence data where a policy document is not a specific requirement. The information supplements our primary privacy notice which can be viewed here; privacy notice and staff privacy notice staff privacy notice

2. Scope

2.1 This policy applies to all personal 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 special category information processed by the GMCA on behalf of other organisations.

2.2 Personal data is defined as: 'any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA…)

2.3. 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.

2.4. This policy applies to data processing where the GMCA is a data controller in its own right or is a data controller in relation to a multi-agency data sharing partnership. This policy also applies when the GMCA is acting as a data processor on behalf of one or more data controllers.

3. Policy Statement

3.1. Data Protection legislation governs how the GMCA will process personal and special category data including, where applicable criminal conviction data, collected from members of the public, current, past and prospective employees, clients and customers, law enforcement and other agencies.

3.2. This policy states how GMCA will comply with UK applicable Data Protection legislation to ensure that all special category and criminal conviction data held is collected, stored and used appropriately.

3.3 Any breach of this policy may result in disciplinary proceedings and/or criminal prosecution.

4. Special category data

4.1 The GDPR defines Special Category data as personal data that reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

5. Criminal conviction data

5.1 While not formally defined as special category data similar additional conditions and requirements also apply to criminal convictions and offences or related to security measures under Article 10 GDPR.

5.2 Section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. When processing such data GMCA will ensure the relevant additional conditions and requirements are met.

6. Roles and Responsibilities

6.1. 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 Chief Executive's liability with regards to offences committed under the Act.

6.2. 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.

6.3. 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 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.

6.4. 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 closely involvedin 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) are 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 you're the organisation so that they can receive essential support, input or information is provided.
-

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

6.5. Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are appointed at the appropriate level of seniority for their service area. Their 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 understand and address risks to information.
- ensuring 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.

6.6. 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)
- acting as gatekeeper ensuring that the Information Asset Owner is aware of any changes to the information asset or its use

6.7. Information Security Officer

The Information Security Officer is responsible for developing and implementing the GMCA Information Security Management System 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 Chief Information Officer.

6.8. 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.

6.9. 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 undertake GMCA's data protection training every year.

6.10. All staff must:

- follow this policy for all processing of personal data including special category and criminal conviction information throughout the GMCA.
- protect any personal data 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 personal 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

6.11. Information Governance Team 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 including special category and criminal conviction information
- provide strategic oversight to large scale programmes of personal data including special category and criminal conviction information sharing
- advise on and provide support in relation to data protection and the handling and use of personal data including special category and criminal conviction information.
- 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.

7. Conditions for processing special category and criminal offence data

7.1 Schedule 1 of DPA 2018 establishes conditions that permit the processing of the special categories of personal data and criminal convictions data.

The GMCA in the processing of such data rely on the following conditions:

7.2 Part 1 – Conditions relating to employment, social security and social protection

The GMCA will process:

Personal data including special category information concerning health in connection with our obligations under employment law and to support employees in their work environment.

We may also process data relating to criminal convictions under Article 10 GDPR in connection with our obligations under employment law in connection with recruitment, disciplinary processes or dismissal.

Examples of processing include staff sickness absences and political activity declarations.

7.3 Part 2 – Substantial Public Interest Conditions

7.3.1 Statutory etc. and government purposes

- Fulfilling obligations under UK legislation for the provision, evaluation and financial/contractual monitoring of services funded by the GMCA for residents within Greater Manchester.
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.

7.3.2 Equality of opportunity or treatment

- Ensuring compliance with the GMCA's obligations under legislation such as the Equality Act 2010.
- Ensuring that we fulfil our public sector equality duty when carrying out our work.
- Ensuring we provide equal access to our services, to all sections of the community in recognition of our legal and ethical duty to represent and serve communities.

7.3.4 Preventing or detecting unlawful acts

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the GMCA and the communities of Greater Manchester.
- Carrying out enforcement action in connection with the GMCA's statutory duties.
- Protecting the public against dishonesty etc.
- Processing data concerning dishonesty, malpractice, or other improper conduct in order to protect the residents of Greater Manchester.
- Carrying out enforcement action in connection with the GMCA's statutory duties, like the Regulatory Reform (Fire Safety) Order 2005
- Carrying out investigations and disciplinary actions relating to our employees.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
- Complying with the GMCA's enforcement obligations under UK legislation, like the Regulatory Reform (Fire Safety) Order 2005.
- Assisting other authorities in connection with their regulatory requirements.

7.3.5 Preventing fraud

- Disclosing personal data including special category and criminal conviction information in accordance with arrangements made by an anti-fraud organisation.

7.3.6 Support for individuals with a particular disability or medical condition

- To provide services or raise awareness of a disability or medical condition in order to deliver services to service users and their carers.

7.3.7 Counselling

- For the provision of confidential counselling, advice or support or of another similar service provided confidentially.

7.3.8 Safeguarding of children and individuals at risk

- Protecting vulnerable children and individuals from neglect, physical, mental or emotional harm.
- Identifying individuals at risk whilst providing services and/or attending emergency incidents.
- Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

7.3.9 Safeguarding of economic well-being of certain individuals

- To protect the economic wellbeing of an individual at economic risk who is aged 18 or over.
- Identifying individuals at risk whilst providing services and/or attending emergency incidents.
- Data sharing with our partners to assist them to support individuals.

7.3.10 Insurance

- Information that is necessary for insurance purposes

7.3.11 Occupational pensions

- Fulfilling the GMCA's obligation to provide an occupational pension scheme.
- Determining benefits payable to dependents of pension scheme members.

7.4 Part 3 – Additional Conditions Relating to Criminal Convictions, etc.

Extension of conditions in Part 2 of Schedule 1 DPA 2018 referring to substantial public interest.

The GMCA may process personal data relating to criminal convictions in connection with its service obligations or as part of recruitment and employment checks to protect the public against dishonesty.

8. Procedures for ensuring compliance with the Principles

8.1 Accountability principle

8.1.1 The GDPR states that the data controller must be responsible for, and be able to demonstrate, compliance with the data protection principles. The Data Protection Officer and Senior Information Risk Owner are responsible for ensuring that the GMCA is compliant with these principles.

8.1.2 The GMCA will:

- ensure that records are kept of all personal data including special category and criminal conviction information processing activities and that these are provided to the Information Commissioner on request
- carry out a Data Protection Impact Assessment for any high risk personal data processing and consult the Information Commissioner if appropriate
- appoint a Data Protection Officer to provide independent advice and monitoring of the GMCA's personal data including special category and criminal conviction information handling and that this person has access to report to the highest management level of the department
- have in place internal processes to ensure that personal data including special category and criminal conviction information is only collected, used or handled in a way that is compliant with data protection law
- Ensure all employees receive annual data protection and information security training
- maintain logs of security incidents, data protection rights requests and details on information sharing with partners
- maintain a data protection policy that sets out how we will ensure we meet our obligations under the GDPR and DPA 2018.

8.2 Principle 1: Lawfulness, Fairness and Transparency

8.2.1 Processing personal data including special category and criminal conviction information must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1 DPA 2018.

8.2.2 GMCA will:

- ensure that personal data including special category and criminal conviction information is only processed where a lawful basis applies,
- only process personal data including special category and criminal conviction information fairly, and will ensure that data subjects are not misled about the purposes of any processing
- ensure that data subjects receive details on why we use and collect their data by providing privacy notices for services, so that any processing of personal data including special category and criminal conviction information is transparent, as well as being clear and easy to understand

8..2.3 Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on the GMCA by the GMCA Orders or any other enactment (whenever passed or made)

8.2.4 Our processing for the purposes of employment relates to our obligations as an employer.

8.2.5 We also process special category personal data to comply with other obligations imposed on the GMCA in its capacity as a public authority e.g. the Equality Act 2010.

8.3 Principle 2: Purpose Limitation

8.3.1 Personal data including special category and criminal conviction information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

8.3.2 The GMCA will:

- only collect personal data including special category and criminal conviction information for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice
- not use personal data including special category and criminal conviction information for purposes that are incompatible with the purposes for which it was collected. If we do use personal data including special category and criminal conviction information for a new purpose that is compatible, we will inform the data subject first

- if we are sharing data with another controller, document that they are authorised by law to process the data for their purpose.

8.3.3 We process personal data including special category and criminal conviction information for purposes of substantial public interest when the processing is necessary for us to fulfil our statutory/public functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement.

8.3.4 The GMCA is authorised by law to process personal data including special category and criminal conviction information for these purposes. We may process personal data including special category and criminal conviction information collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

8.4 Principle 3: Data Minimisation

8.4.1 The GMCA will only collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The GMCA will only collect the minimum personal data including special category and criminal conviction information that we need for the purpose for which it is collected.

8.4.2 Where personal data including special category and criminal conviction information is provided to us or obtained by us, but is not relevant to our stated purposes, this will be erased.

8.5 Principle 4: Accuracy

8.5.1 GMCA will ensure that personal data including special category and criminal conviction information is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data including special category and criminal conviction information has a significant impact on individuals.

8.5.2 Where the GMCA become aware that personal data including special category and criminal conviction information is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

8.5.3 The GMCA will also maintain a Data Quality Policy that sets out the processes we will follow to ensure our data is of the highest quality possible.

8.6 Principle 5: Storage Limitation

8.6.1 Personal data including special category and criminal conviction information shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data including special category and criminal conviction information are processed.

- GMCA will only keep personal data including special category and criminal conviction information in identifiable form for as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data, it shall be deleted or rendered permanently anonymous. GMCA will maintain appropriate Data Retention and Disposal Policies and Schedules.
- Retention periods are set out in our Retention and Disposal Schedules and are published in our Records of Processing Activities Register and Privacy Notices
- Retention periods are based on legal requirements to retain data and consideration of the needs of data subjects through data protection impact assessments.

8.7 Principle 6: Integrity and Confidentiality (security)

8.7.1 Personal data including special category and criminal conviction information shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8.7.2 GMCA will ensure that there are appropriate organisational and technical measures in place to protect personal data. We do so in the following ways.

- We adhere to the Government's Minimum Cyber Security Standards and implements information security controls in line with Public Sector Network, Payment Card Industry and the NHS Data Security and Protection Toolkit
- The Greater Manchester Information Governance Board meets regularly to ensure suitable information governance is deployed throughout the GMCA.
- Employees looking after our IT network are vetted in line with HMG Baseline Personnel Security Standard.
- Technical security controls such as encryption are employed to secure sensitive information within systems.
- Role-based access controls are implemented to restrict access to sensitive data.
- Where possible, anonymisation or pseudonymisation techniques are used to reduce the risk of sensitive data being compromised. Please see our separate anonymisation and pseudonymisation policy for more information on how we do this.
- Retention and erasure policies are in place to ensure data is retained in line with agreed retention periods, and securely disposed of when appropriate.

- We retain personal information only for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

8.7.3 The GMCA will ensure, where special category or criminal convictions personal data is processed, that:

- there is a record of that processing, which complies with the requirements of Article 30 GDPR and paragraph 41 of Schedule 1 of the DPA and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data;
- where we no longer require special category or criminal convictions personal data for the purpose for which it was collected, we will delete it or render it permanently anonymous;
- all contracts with data processors include clauses regarding the exit of the contract and the return or destruction of any special category or criminal convictions personal data processed.
- data subjects receive full privacy information about how their data will be handled, and that this will include the period for which the special category or criminal convictions personal data will be stored, or if that is not possible, the criteria used to determine that period.
- we retain personal information only for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

9. Review

9.1 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. .

9.2 This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

10. Training and Awareness

10.1 Staff will be made aware of this policy by it being hosted on the Information Governance section of the GMCA intranet.This policy will also be published on the GMCA website.

10.2 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.

10.3 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.

11. Compliance and Monitoring

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

11.2 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.

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

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

11.5 Staff are responsible for informing the Information Governance Team of any new processing or changes to existing processing of personal data including special category or criminal conviction information within their area. This will help the GMCA ensure it meets the requirements of Data Protection legislation.

12. Data Protection Officer

12.1 **Phillipa Nazari Data Protection Officer**; Assistant Director Information Governance

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

Email: OfficeofDPO@greatermanchester-ca.gov.uk

13. General Enquires

13.1 **Information Governance Team;** Greater Manchester Combined Authority, Churchgate House, 10, Oxford Street, Manchester M1 6EU

Email: OfficeOfDPO@greatermanchester-ca.gov.uk

Policy: Data Subjects Rights 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

Document Version Control 2
1. Introduction 5
2. Scope 6
3. Policy Statement 6
4. Roles and Responsibilities 6
4.1. Chief Executive 6
4.2. Monitoring Officer 7
4.3. Senior Information Risk Owner (SIRO) 7
4.4. Data Protection Officer (DPO) 7
4.5. Information Asset Owners (IAOs) 8
4.6. Information Asset Administrators (IAA) 8
4.7. Information Security Officer 9
4.8. Heads of Department: 9
4.9. Line managers 9
5. Introduction to data subject rights 10
6. Data subjects have the following rights: 10
7. Summary of your Rights – what these are and how they apply 12
7.1. Right to be informed 12
7.5. Right of Access 12
7.6. Right to rectification 13
7.7. Right to object to processing 14
7.8. Right to restriction of processing 15
7.9. Right to erasure (‘Right to be forgotten’) 16
7.10. Right to data portability 17
7.11. Rights relating to automated decision-making 17
8. How individuals can exercise these rights 18
8.1 How do individuals make a request about any of their rights? 18
8.2 Can someone else make a request for the individual? 19
8.3 What if a data subject ‘lacks mental capacity’? 19
8.4 What about requests involving children? 19
8.5 How do individuals evidence parental responsibility? 20
8.6 When can individuals expect your response? 20
8.7 What will we send the individual when we respond? 21

8.8 Will individuals have to pay a charge? 21
8.9 Will individuals get all of the information they are requesting? 21
8.10 Can individuals choose the format in which their information is supplied? 22
8.11 Can GMCA refuse requests? 22
8.12 What if individuals am not satisfied with our response or it is taking too long? 22
9. Training 23
10. Compliance and Monitoring 23
Appendices 25
Appendix 1: Definitions 25
Appendix 2 Further Information and Guidance 27

1. Introduction

1.1 The Greater Manchester Combined Authority (GMCA) was established in April 2011 and since 2017 also has in place the elected Mayor of Greater Manchester who works collaboratively with other public sector organisations, voluntary and private enterprises in order to improve the GM region and the lives of all its citizens, by encouraging economic growth, facilitating public sector reform and delivering the Greater Manchester Strategy.

1.2 The GMCA's remit across Greater Manchester includes:

- Fire and rescue
- Police, crime and justice
- Waste
- Education skills and training
- Economic development
- Regeneration and housing
- Strategic spatial planning
- Research, data analysis and evaluation
- Digital strategy
- Facilitating public service reform

1.3 In order to fulfil its functions and duties as a Combined Authority the GMCA collects and processes personal data relating to individuals who use the services it provides, past, present and prospective employees, contractors, suppliers, clients, and others with whom it communicates.

1.4 Not only does the GMCA collect and process personal data for the day to day running of the Authority but also to fulfil its wider role as a commissioner of services, for providing fire and rescue services across the region, as the Police and Crime Commissioner for Greater Manchester, for supporting the Mayoral Office, in undertaking research and consultations with the public and working together with its strategic partners to facilitate public sector reform and deliver the Greater Manchester Strategy.

1.5 The GMCA is responsible for being instrumental in the strategic changes required across GM to enable increased information sharing across public service delivery for public benefit. It is therefore imperative that organisational compliance with Data Protection laws for the GMCA is one that is continually striving for excellence.

1.6 This policy therefore sets out how the GMCA will comply with the Data Protection legislation in order to ensure that data subject rights are adhered to.

1.7 Any breach of this policy may result in disciplinary action and prosecution.

2. Scope

2.1 This policy applies to all personal information including 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 personal information and special category information processed by the GMCA on behalf of other organisations.

2.2 Personal data is defined as:

‘any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA…)

2.3 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 Data Protection legislation governs how the GMCA will process personal and special category data including where applicable criminal conviction data collected from members of the public, current, past and prospective employees, clients and customers, law enforcement and other agencies.

3.2 This policy states how the GMCA will comply with Data Protection legislation to ensure that data subject rights are adhered to.

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.

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 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 Head of Information Governance.

4.5. Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are members of the Extended Leadership Team.

Their 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.

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

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. Directors:

Directors 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.

4.9. Line managers

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.
- All staff must:
- Follow this policy for all processing of personal data throughout the GMCA.
- Protect any personal data 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 personal 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
- 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.

5. Introduction to data subject rights

5.1. The rights of individuals ('data subjects') in relation to the processing of their personal information are set out in data protection legislation.

5.2. The General Data Protection Regulation (GDPR) strengthened rights which already existed in UK law. The changes are mostly evolutionary but also give individual's rights in other areas such as the right to data portability. Some of these rights are subject to limitations and exceptions; further details of which may be viewed below.

5.3. This guidance provides an introduction to the rights individuals have under the data protection legislation.

5.4. Information and advice can be obtained from the Greater Manchester Combined Authority's Information Governance Team; OfficeOfDPO@greatermanchester-ca.gov.uk

6. Data subjects have the following rights:

- **The right to be informed** - The right to be provided with specified information about the processing of their personal data.

- **The right of access** - The right to access their personal data and certain supplementary information.

- **The right to rectification** - The right to have their personal data rectified, if it is inaccurate or incomplete.

- **The right of erasure / right to be forgotten** - The right to have, in certain circumstances, their personal data deleted or removed.

- **The right to restriction** - The right, in certain circumstances, to restrict the processing of their personal data.

- **The right of data portability** - The right, in certain circumstances, to move personal data the individual has provided to the GMCA to another organisation.

- **The right to object** - The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the GMCA to stop processing that data.

- **Rights related to automated decision making and profiling** - The right to not be subject to decision-making based solely on automated processing.

6.2. Please be aware that these rights are not absolute and are subject to conditions and exemptions. In some cases the rights described above only apply if the processing activity is undertaken on specific legal grounds and/or in defined circumstances. Therefore all of these rights are unlikely to be engaged in all cases.

6.3. Individuals can also obtain full information about their rights from the Information Commissioner's Office (the ICO) via their website: https://ico.org.uk/your-data-matters/.

6.4. The ICO is the UK's independent regulator responsible for upholding and enforcing the rights of individuals under data protection law.

6.5. Where an individual exercises their individual rights listed above, the Greater Manchester Combined Authority ('The GMCA') will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:

- Further time may be necessary, taking into account the complexity and the number of the request(s) from the individual, the period for responding may be extended by up to two further calendar months. Where such an extension is required The GMCA will notify the individual that this is the case within one calendar month of receiving their request.

- Where the request(s) from an individual are manifestly unfounded or The GMCA may refuse the request(s). In exceptional cases a reasonable fee may be requested that takes into account the administrative cost of complying with the request.

7. Summary of your Rights – what these are and how they apply

7.1. Right to be informed

The GMCA will ensure that

- where we collect personal data from the individual we will provide them with, at the time the personal data is collected, specified 'fair processing' information (known as a 'privacy notice')

- where we use personal data that has not been collected directly from the individual to communicate with them, we will provide the privacy notice, at the latest, when the first communication takes place;

- if we plan to disclose personal data that has not been collected directly from the individual to another recipient, we will provide the privacy notice, at the latest, before the data are disclosed.

7.2. Each time we seek to collect information from the individual, we must inform them why we need to process theirpersonal information, including how we propose to use it, who we intend to share it with and the safeguards we have put in place.

7.3. Further information relating to the use of personal data may be viewed on our Privacy Policy, which can be viewed at https://www.greatermanchester-ca.gov.uk/who-we-are/accounts-transparency-and-governance/privacy-policy-and-data-protection/

7.4. Further to this, the individuals also have the right to be informed of any significant data breach of their personal information. The reporting must be done without undue delay unless there are relevant reasons why they should not be informed, e.g. disclosure of the breach would cause them harm.

7.5. Right of Access

Individuals are entitled to ask us for copies of the personal information that we hold about them.

The right of access also extends to

- Receiving confirmation from the GMCA whether or not we are processing their personal data; and, if it is
- To be given access to the personal data, including the right to a copy of the personal data;
- To be informed of the purposes of the processing of the personal data;
- To be informed of the categories of the personal data being processed;

- To be informed of the recipients or categories of recipient to whom the personal data have been or will be disclosed;
- To be informed of the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- To be informed of the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the individual or to object to such processing;
- To be informed of the right to lodge a complaint with the ICO (see section 4.12);
- To be able to contact and make complaints directly to the Data Protection Officer (see section 2);
- To be provided with, where we have not collected the personal data from you, any available information as to their source;
- To be informed of the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them;
- Where personal data are transferred to a third country or to an international organisation, they have the right to be informed of the appropriate safeguards under the data protection legislation relating to the transfer.

The individual should provide us with as much detail as theycan about the information they want to access. This will allow us to undertake precise searches, and locate the information at the earliest opportunity. It's possible that should we need to contact the individual for further information to help us find the personal data they requested they may have to wait longer for a response.

7.6. Right to rectification

The individuals are entitled to ask us to:

- correct inaccurate information about them;
- update the information we hold if it is incomplete

If we agree that the personal information they have identified is factually inaccurate, we will correct it.

The GMCA will:

- endeavour to inform anyone with whom we may have shared the individuals personal information of any correction(s) we have made so they can rectify the information they hold about them;

- tell the individual who the recipients of their information are if they ask us to do this so the individual can check the recipient has updated the personal information they hold about them.

7.7. Right to object to processing

Individuals have the right to object to us using their personal information where it is being processed for:

- direct marketing;
- profiling whether linked to direct marketing or for other purposes
- performing our statutory functions, tasks carried out in the public interest or when exercising official authority;
- our legitimate interest or those of a third party;
- scientific/historical research/statistics where:
    - this is likely to cause substantial damage or substantial or distress; or
    - involves decision-making about an individual

If they object to us using their personal information for direct marketing (or profiling linked to direct marketing) we will cease processing for this purpose(s) as soon as possible and no longer than 28 days after the individual has made the complaint. The GMCA will only use your personal data for direct marketing if the individuals have actively chosen to opt in to this service. If we intend to collect their personal data with the intention or expectation that we will send marketing material to them, we must tell them about this in advance and give them the chance to opt in to receiving such communications. If the individual has opted in and later decides that they no longer wish to receive marketing communications, we will not continue to hold their personal data for marketing purposes.

Where the individual makes an objection in relation to the processing of their personal information for public task/legitimate interests, this must be on grounds relating to their "particular situation". The GMCA must then cease the processing of the individual's personal data, unless

- we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual; or
- the processing is for the purposes of the establishment, exercise or defence of legal claims.

If the individual objects to the use of their personal data for scientific/historical research or statistical purposes on one or both of the above grounds, we will carefully consider their request and let them know the outcome. It may not always be possible to meet their objection if for example, the processing is carried out for the purpose of measures or decisions with respect to particular individuals where this is in accordance the law and is necessary for specified bodies to carry out approved medical research.

Where the individual objects to us processing their personal information for any of the other reasons above, we will:

- consider if we have compelling legitimate grounds for continued processing; and
- whether or not these grounds are sufficiently compelling to justify overriding the individuals privacy rights.

Where the law requires us to process their information to meet our statutory functions and

public tasks, including our law enforcement functions, it is very likely that we will not be able to comply with the individuals request.

For example, they will not be able to use this right to prevent us from:

- taking measures to protect the health and safety of our staff;
- establishing, exercising or defending our legal rights;
- pursuing criminal investigations or proceedings;

The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.

The Greater Manchester Combined Authority may collect health data in order to deliver specific services. The National Data Opt-out means that members of the public can decide that they do not want their information using for anything other than providing care or a direct service to them where the law does not specifically say it can be used in this way.

There are now rules in place concerning secondary use of health and social care data. This is when personal data is used for purposes not involving direct care, for example for research and planning purposes.

All health and care organisations are now required to respect these decisions and comply with the National Data Opt Out. The Greater Manchester Combined Authority may not hold any data that the opt-out would apply to but needs to assess this on a case by case basis.

For further information; https://digital.nhs.uk/services/national-data-opt-out

7.8. Right to restriction of processing

This right may be exercised in circumstances where:

- we need time to consider the individuals representations where they are:
    - contesting the accuracy of the personal information we hold about them; or
    - objecting to our processing of their information (see previous right)
- it has already been determined the processing is ‘unlawful’ and theyask us to retain and ‘restrict’ its use;
- we no longer need to retain their personal information but they ask us to retain it for the establishment, exercise or defence of own legal claims.

If an individual makes a request we will let them know if we agree to restrict access to their information for one or more of the above reasons.

If we decide a restriction is appropriate, we will attempt to notify any recipients of their personal information of the restriction and let the individual know who they are if they ask us to do so.

Where processing is restricted, as well as storing the individals personal information, we will only process it during the period of restriction:

- with their consent; or
- if it is necessary for the establishment, exercise or defence of legal claims;
- if it is necessary for the protection of the rights of another person; or
- if it is necessary for reasons of important public interest, including for example, communicating with the Information Commissioner.

Where a restriction is applied pending a determination of 'accuracy' or any 'objection' the individual may have submitted, we will let them know the outcome of their representations and will notify them prior to lifting the restriction.

Where the reason for the restriction is for one of the other reasons above, the erasure of the personal information will not take place until we have resolved evidential issues with the individual.

We must inform the individual if we decide to lift any restrictions placed on the processing of their data. They should receive this notification before we lift this restriction.

Where the GMCA puts a restriction on processing in place and has previously disclosed the data to others, we must inform each recipient of the restriction (unless this is impossible or would involve disproportionate effort).

7.9. Right to erasure ('Right to be forgotten')

Individuals have the right to request that we erase their personal information in defined circumstances.

These defined circumstances are:

- if we are storing their personal information for longer than is necessary or in breach of a legal obligation that requires its erasure;
- they decide to withdraw their consent and ask us to erase their personal information where there is no other legal ground for processing;
- we have accepted an objection made by them to our processing of their personal information (see 3.4 above) and they have further requested that we erase the personal information in question;
- we are processing or publishing their personal information without a legal basis for doing so;
- where we are legally obliged to erase the information; or
- the personal data was collected in relation to an offer of an information society service (in other words, for a fee over the internet) to a child.

We will carefully consider a request for erasure. Our response will outline whether or not we consider retention of their personal information is unwarranted.

Please note that erasure or the "right to be forgotten" is not an absolute right. There are circumstances where it may not always be possible to agree to the individual's erasure request and we have listed a number of grounds below where it may be necessary for us to retain their information:

- in the interests of freedom of expression (special journalistic purposes)
- in order to comply with a legal obligation;
- for archiving in public interest;
- for public health functions in public interest
- for exercising legal rights or defending legal claims

If we agree to erase their personal information, we will attempt to notify any recipients and let them know who they are if the individual ask us to do so (unless this is impossible or would involve disproportionate effort). If the GMCA has previously made their personal information public, we will also attempt to inform other data controllers who are processing the data that they have requested their erasure (although this will depend on the technical availability and cost of informing them of the request).

7.10. Right to data portability

In certain circumstances, individuals have the right to request that the personal information they have supplied to an organisation be converted into a structured, commonly used and machine-readable format (e.g. a CSV file) so that it can be transmitted to another organisation. This right is primarily intended to stimulate competition in the commercial sector by making it easier for consumers to switch from one supplier to another.

As most of the processing activities undertaken by us are governed by statute or as a result of legal obligations imposed on us, this right will only be engaged where:

- The individual has provided the personal information to us themselves, we are processing it on an automated basis, and the legal basis for our processing:

    - is based on their consent; or
    - is for entering into or the performance of a contract with them.

If they make a request for the personal information they have supplied to us to be converted into a portable format where our legal basis for processing falls within one of the grounds above, we will let them know our decision. We will be unlikely to agree to requests to transfer personal data that concerns other individuals, especially when providing the information will impact on the rights of those individuals or prejudice them in some way.

If we agree to their request, we will transfer the personal data in question directly to the other data controller they have identified, provided that such a transfer is technically feasible. However, we are not required to adopt or maintain processing systems that are compatible with those of other data controllers.

7.11. Rights relating to automated decision-making

In general, decisions which effect the individual legally or have similarly significant effects are not permitted using solely automated processing (i.e. decision-making without human involvement), especially if this involves the use of 'Special Category Data'. This is because decisions made using automated electronic programmes or software do not involve human beings.

But there are some exceptions where automated decision-making is permitted. This is where the processing:

- is based on individuals explicit consent;
- is necessary for entering into or the performance of a contract with them;
- it is required or authorised by law

Where an automated decision is made about the individual based on one of the reasons above, they are entitled to be:

- informed that our processing activity involves automated decision making and to be informed about the logic involved and the likely consequences of the processing for them;
- told what measures and safeguards we have implemented to protect their privacy;

Where the GMCA undertakes automated decision making or profiling we will:

- notify individuals about the processing;
- provide a mechanism for them to request that we reconsider the decision or take a new decision that is not based solely on automated decision making;
- carry out regular checks to ensure the automated decision making / profiling is working as intended.

We will only subject individuals Special Category Data to automated decision making or profiling where they have given explicit consent or where the processing is necessary for reasons of substantial public interest.

Within one month of receipt of the above notification, individuals have the right to:

- contest the automated decision; and
- ask that the automated decision be reconsidered by an appropriate person with the authority/seniority to reach a fresh decision that is not based solely on automated processing.

If they contest an automated decision and ask for it to be reconsidered, we will respond within the allowed time period and let them know whether or not this fresh decision has led to the same or a different outcome.

8. How individuals can exercise these rights

8.1 How do individuals make a request about any of their rights?

Individuals can exercise any of the data subject rights mentioned in this policy by writing to the GMCA Information Governance Team at: officeofdpo@greatermanchester-ca.gov.uk.

To help them to understand how the GMCA processes their data in order to exercise any of their rights, we explain on our website how we collect and use personal information about them, including the types of information we process, what we will do with their information, who we may share it with, the 'lawful bases' (conditions) for processing it, and a list of our 'legal obligations' (powers) to use their personal data to provide services to you. They can view this page at https://www.greatermanchester-ca.gov.uk/who-we-are/accounts-transparency-and-governance/privacy-policy-and-data-protection/.

Further information in relation to submitting a Subject Access request via GMFRS may also be found via the following link; https://manchesterfire.gov.uk/about-us/publication-scheme/subject-access-request/

For **all** requests, we will need documentary proof that they are who they say they are. This is for security reasons to ensure we are dealing with the individual and that none of their personal information is accessed or interfered with by anyone else falsely claiming to be them.

Individuals need to ensure they provide at least two forms of identification. Preferably a copy of a passport, driving licence, utility bill, council tax bill or bank statement bearing their full name and current postal address.

On receipt of their request, we will send them a written acknowledgement. In some circumstances we may also ask for additional information if necessary.

8.2 Can someone else make a request for the individual?

Individuals can ask anyone to act on their behalf. For example a friend, relative, solicitor or employee of a consumer organisation such as a Citizens Advice Bureau.

However, before we discuss or provide the individuals personal data to anyone acting on their behalf the individual must confirm to us in writing that they have their authority to do so. This will require the individiuals signed authority, coupled with two forms of identification.

8.3 What if a data subject 'lacks mental capacity'?

A person with a lasting power of attorney appointed directly by the data subject or a Deputy appointed by the Court of Protection may exercise rights on behalf of the data subject.

8.4 What about requests involving children?

It is important to remember that personal data about a child, however young, is the child's personal data and is not the personal data of their parent or guardian.

A parent or guardian does not have an automatic right to personal data about their child and can only apply on the child's behalf if the child:

• has given consent; or
• is too young to have an understanding to make the application.

Unlike Scotland, there is no set age in England which recognises when children are automatically able to exercise data protection rights.

A child aged 13 or over is able to create an on line social media account without the consent of a person with parental responsibility.

As a general rule a child must have sufficient understanding and maturity to exercise their own rights and a common sense approach will be adopted in the event a child or young person submits a request.

For children aged under 13, it will generally be expected that a request is made by a person with parental responsibility. A ‘best interest’ consideration will be taken into account.

Individuals have the right to request that we erase personal data that was collected in relation to an offer of an ‘information society service’ to a child (see section 3.4).

8.5 How do individuals evidence parental responsibility?

The following evidences may be accepted as proof of parental responsibility:

- Birth Certificate
- Court Order
- Adoption Record
- Special Guardianship Order

8.6 When can individuals expect your response?

We aim to respond to requests without undue delay and no later than one calendar month counted from the first working day after we are in receipt of an individuals request, and:

- proof of their identity, **and**
- any further information (where we have requested this from them) we need to process their request and/or locate and retrieve their personal information.

Where it is not possible to respond sooner and the last day before expiry of one calendar month, falls over a weekend or on a bank holiday, the latest due date will be treated as the first working day after the weekend or bank holiday.

If a request is complex, we may need to extend the length of time required to respond.

If this applies, we will let the individual know before the latest due date on which they would

be expecting to hear back from us.

Data protection legislation says we can extend the length of time to respond by a maximum of a further two calendar months.

Where it is not possible to respond sooner and the last day before expiry of the second calendar month, falls over a weekend or on a bank holiday, the latest due date will be treated as the first working day after the weekend or bank holiday.

We will always try to respond as quickly as we can.

8.7 What will we send the individual when we respond?

At the time of fulfilling the request, alongside copies of any information about the individual which they have requested and we are able to disclose, we will also provide the following information:

- the reasons why it is necessary to process their personal information;
- the types of personal information we process;
- the recipients or categories of recipient to whom their personal information have been or will be disclosed, including any recipients in third countries or international organisations and if relevant, the safeguards applicable to the transfer;
- where possible, the envisaged period for which their personal information will be stored, or, if not possible, the criteria used to determine that period;
- the right to request rectification, erasure of personal information or to object or seek to restrict such processing;
- the right to lodge a complaint with a supervisory authority (see section 4.12);
- the source(s) of any personal information we hold that has not been collected directly from them;
- whether or not decisions are made about the individual solely using automated means, including profiling, without human intervention and, if so, provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

8.8 Will individuals have to pay a charge?

Ordinarily we will not charge a fee for fulfilling a request from the individual.

The only exception is where the individual makes repeat requests for the same or similar information. In these cases, we reserve the right to charge a reasonable fee based on the administrative costs of supplying further copies if we consider a reasonable time period has not intervened since fulfilling a previous request.

Where the right of data portability is engaged, we must also provide information through this route free of charge (see section 3.7).

8.9 Will individuals get all of the information they are requesting?

This is likely to be the case.

But it is important to note that the right of access to their own information does not extend to information about other people who may be identified in the information that also refers to them.

GMCA may therefore redact (blank out) personal information about other individuals (called 'third parties' in the data protection laws) where we are satisfied it is reasonable in the circumstances to do so. We may withhold or redact some information the individuals request about themselves where it is possible to identify a third party.

In some cases information may be so interlinked that it is not possible to fulfil their request without breaching another person's privacy rights.

The names of professional staff (whether directly employed by us or not) involved in decision-making about the individuals care and education will often be disclosable and their identities will not be automatically redacted, unless this is warranted in a particular case.

The law recognises that there are occasions when it may be appropriate to withhold certain information and provide exemptions in specified circumstances. For example, it may be exempt if providing it to the individal would compromise the prevention or detection of crime or the prosecution of offenders. In certain cases we may also withhold some information relating to education, health and social work.

If we withhold information on the basis that it is exempt from disclosure, where it is possible to do so, we will explain the exemption(s) we are relying on and the reasons why one or more are necessary.

8.10 Can individuals choose the format in which their information is supplied?

Once we have located individuals personal data we will provide copies to them in the same format they first contacted us, unless specified otherwise.

Where individuals have submitted their request electronically or asked us to respond in a particular format, we will try to do so wherever this is reasonably practicable.

8.11 Can GMCA refuse requests?

In certain circumstances we may refuse to act on individuals request if we consider that theirrequest is unfounded, excessive or repetitive in nature.

We will give our reasons if we refuse to comply with requests on any of these grounds.

8.12 What if individuals am not satisfied with our response or it is taking too long?

Upon receipt of individual's requests we have one calendar month to provide them with a

response, or contact them to tell them how much longer we need to fulfil their request.

The Information Commissioner's Office (ICO) is the UK's independent regulator responsible for upholding and enforcing the rights of individuals under the data protection laws.

If individuals do not hear from us by the latest due date or are not satisfied with the response they have been given, they have the right to complain to the ICO.

If individuals consider that personal information we hold about them is incomplete and we do not agree with this, we may offer them the option of adding a supplementary statement explaining why they consider the information we hold is incomplete.

If we disagree with their view that the information we hold about them is factually wrong, or refuse their request for erasure, then in our response we will explain the basis for our decision and give them details about their right to complain to the ICO if they are not satisfied.

They can contact the ICO

Via their website: https://ico.org.uk/make-a-complaint/.

By post:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

9. Training

9.1. The GMCA will provide relevant training both on line and face to face to ensure that staff understand the legislation and its application to their role.

9.2. 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.

9.3. 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 personal information. Failure to do so may result in disciplinary action and legal prosecution.

10. Compliance and Monitoring

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

10.2. Staff are responsible for informing the Information Governance Team of any new processing or changes to existing processing of personal data within their area. This will help the GMCA to meet the requirements of the legislation.

10.3. This policy will be reviewed at regularly by the Information Governance Team to ensure that it is updated in line with any change in legislation.

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

Appendices

Appendix 1: Definitions

- “Personal information” means any information relating to an identified or identifiable living person. An identifiable person is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier.

- “Special or Sensitive Personal information” is information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal information relating to criminal offences and convictions.

- “Processing” means any activity that involves the use of personal information. It includes obtaining, recording or holding the information, or carrying out any operation or set of operations on the information including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal information to other Recipients.

- “Data Subject” a living, identified or identifiable individual about whom we as the Controller hold personal information.

- “Controller” means the person or organisation (in this case us) that determines when, why and how to process personal information.

- “Privacy Notices” are notices setting out the information given to you at the time we collect information from you or within a reasonable time period after we obtain information about you from someone else. These notices may take the form of an overarching privacy statement (as available on our web site) or apply to a specific group of individuals (for example, service specific or employee privacy notices) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose.

- “Consent” must be freely given, specific, informed and unambiguous indication of an individuals’ wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- “Explicit Consent” requires a very clear and specific statement, leaving no room for misinterpretation.

- “Third Party” is a living individual other than the person who is the data subject

- “Recipient” means a person or organisation who receives your personal information from us. This may be a company with whom we have entered into a contract to provide services on our behalf or another Controller with whom we are

either required or permitted to share personal information.

- “Latest due date” means one calendar month counted from the first working day after proof of ID and any requested information is received by us, except where this falls on a weekend or a bank holiday in which case the “latest due date” is treated as the first working day after the weekend or bank holiday. The same method is applied to calculating the “latest due date” for complex requests where an extension of time is permitted and claimed.

- “Automated Processing” means any processing of personal information that is automated through the use of computers and computer software.

- “Automated Decision-Making (ADM)” means a decision which is based solely on Automated Processing (including Profiling) which produces legal effects or significantly affects an individual. Data protection legislation generally prohibits Automated Decision-Making except in defined circumstances, subject to certain conditions and safeguards being met.

- “Profiling” means the recording and analysis of a person's psychological and behavioural characteristics, so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people.

- “Data protection legislation” has the same meaning as defined in the Data Protection Act 2018, and includes GDPR, the Data Protection Act 2018 and any regulations or secondary legislation made underneath them.

- “General Data Protection Regulation (GDPR)” means the General Information Protection Regulation ((EU) 2016/679).

Appendix 2 Further Information and Guidance

Data Protection Officer

Data Protection Officer – Assistant Director

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

Email: OfficeofDPO@greatermanchester-ca.gov.uk

General enquires and Data Subject Requests

Information Governance Team GMCA, Churchgate House, 10, Oxford Street, Manchester M1 6EU

Email: OfficeofDPO@greatermanchester-ca.gov.uk

Information Commissioner

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Tel: 0303 123 1113

www.ico.org.uk

Online Resources

- ICO – www.ico.org.uk

GMCA intranet https://GMCA Information Security

This page is intentionally left blank

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

Document Version Control 2
1. Introduction 4
2. Scope 4
3. Policy Statement 5
4. Roles and Responsibilities 5
5. The importance of good data quality 8
6. Risk Management 10
7. Data Quality Requirements 11
8. Compliance with data quality principles 12
9. Policy exemption 12
10. Review 13
11. Training and Awareness 13
12. Compliance and Monitoring 13
13. Contact details 14

Appendix 15
Appendix 1 - Legislative Framework 15

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.

This page is intentionally left blank

GMCA GREATER MANCHESTER COMBINED AUTHORITY

RESOURCES COMMITTEE

Date: 30 July 2021

Subject: GMCA Information Governance Policies

Report of: Eammon Boylan, Chief Executive

PURPOSE OF REPORT

The report presents a set of information governance policies for GMCA that will provide a clear framework for employees, ensuring that they understand their role in supporting the GMCA's organizational compliance.

RECOMMENDATION

The Committee is asked to approve the appended information governance policies:

- Appropriate Policy (Special Category Data)
- Data Subject Rights Policy
- Data Quality Policy
- Anonymization and Pseudonymization Policy
- Freedom of Information and Environmental Information Regulations Policy.

CONTACT OFFICERS:

Steve Wilson – GMCA Treasurer and Senior Information Risk Owner
steve.wilson@greatermanchester-ca.gov.uk

Phillipa Nazari – Assistant Director Information Governance and Data Protection Officer
phillipa.nazari@greatermanchester-ca.gov.uk

1.0 BACKGROUND

1.1 Data protection law specifically requires organisations to put in place effective data protection policies, to enable them to take the practical steps to comply with their legal obligations. The Data Protection Act came into force in thew UK in 2018. It outlines that employees can face prosecution for data protection breaches. As with previous legislation, the new law contains provisions making certain disclosure of personal data a criminal offence.

1.2 The following set of GMCA organizational policies are intended to provide clarity and consistency for employees, by communicating what people need to do and why, to help them avoid the potentially serious, criminal implications for employees that can arise from failure to comply with data protection legislation. Examples from the Data Protection Act (2018) include:

Section 148: Destroying or falsifying information and documents etc. (Data Quality). Under Section 148 (2) (a) it is an offence for a person to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material.

Section 173: Alteration etc. of personal data to prevent disclosure to data subject (Data Subject Requests).

Section 173 relates to the processing of requests for data from individuals for their personal data. Section 173 (3) makes it a criminal offence for organisations (persons listed in Section 173 (4)) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure.

Section 171: Re-identification of de-identified personal data (anonymization and pseudonymization)

Section 171 - a new offence - criminalizes the re-identification of personal data that has been 'de-identified' (de-identification being a process - such as redactions - to remove/conceal personal data). Section (5) states that it is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified.

1.3 In relation to the Freedom of Information Act (2000) Section 77 states a person "*is guilty of an offence if he alters, defaces, blocks, erases, destroys or conceals any record held by the public authority, with the intention of preventing the disclosure by that authority of all, or any part, of the information to the communication of which the applicant would have been entitled*."

1.4 The attached policies have been drafted by the GMCA Information Team in conjunction with the GMCA Information Governance (IG) Board. The Freedom of Information and Environmental Information Regulations Policy was considered and agreed with Trade Unions representatives in October 2020.

1.5 All policies follow an agreed format and style, including arrangements for document version control.

2.0 APPROPRIATE POLICY (SPECIAL CATEGORY DATA)

2.1 As part of the Greater Manchester Combined Authority's (GMCA) statutory and public functions, it processes special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

2.2 This policy applies when the GMCA is processing special category data when relying on the requirements listed in Parts 1, 2 and 3 of Schedule 1 of the Data Protection Act 2018. This policy lists the procedures, which are in place to secure compliance with the General Data Protection Regulation and data protection principles, needed when processing special category data. It applies to all GMCA staff. "Staff" for the purposes of this policy includes GMCA officers, including contractors, consultants and agency staff.

2.3 The Appropriate Policy (Special Category Data) is attached as appendix 1.

3.0 DATA SUBJECT RIGHTS POLICY

3.1 This policy provides an introduction to the rights individuals have under the data protection legislation.

3.2 The rights of individuals ('data subjects') in relation to the processing of their personal information are set out in the General Data Protection Regulation (GDPR). Further provisions relating to the data rights of individuals can be found within the Data Protection Act 2018 (DPA 2018), which include law enforcement activities and other areas not covered under the GDPR.

3.3 The GDPR strengthens these existing rights. The changes are mostly evolutionary but also give individual's rights in other areas such as the right to data portability. Some of these rights are subject to limitations and exceptions; further details of which may be viewed below.

3.4 The Data Subject Rights Policy is attached as appendix 2.

4.0 DATA QUALITY POLICY

4.1 The Greater Manchester Combined Authority (GMCA) recognizes that reliable information is essential and the availability of complete, accurate, relevant, accessible and timely data is fundamental in supporting the GMCA to achieve its goals. The GMCA recognizes that all decisions, whether service delivery, performance management, managerial or financial need be based on information which is of the highest quality.

4.2 The data quality 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.

4.3 The Data Quality Policy is attached as appendix 3.

5.0 ANONYMISATION AND PSEUDONYMISATION POLICY

5.1 Effective pseudonymization and/or anonymization processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality. They are part of the Data Protection by Design approach (Article 25 of GDPR) through which data protection is integrated into processing activities and business practices, from the design stage right through the lifecycle. They will often be relevant to a Data Protection Impact Assessment (DPIA) and form a key technical measure to ensure processing complies with the data protection principles (Article 35 of GDPR).

5.2 This policy therefore sets out how the GMCA will comply with the Data Protection legislation in order to ensure that the personal data it holds is used appropriately, processed safely and securely and that individuals are able to exercise their rights.

5.3 The Anonymization and Pseudonymization Policy is attached as appendix 4.

6.0 FREEDOM OF INFORMATION AND ENVIRONMENTAL INFORMATION REGULATIONS POLICY

6.1 As an organization, one of the most frequent types of requests we receive are Freedom of Information requests. In order to support the organization in managing these requests, and in order to ensure that we are compliant to Data Protection Act 2018, General Data Protection Regulation and Freedom of Information Act 2000 we have produced new guidance which includes a policy, procedure, frequently asked questions and a guide to exemptions.

6.2 This policy sets out our organizational approach to Freedom of Information and Environmental Information Regulation requests. The policy has been approved by the Unions.

6.3 The Freedom of Information and Environmental Information Regulations Policy is attached as appendix 5.

7.0 NEXT STEPS

7.1 Subject to approval of the policies by this Committee, an updated training offer for employees will be delivered alongside a communications plan (both for all employees and key stakeholders) to ensure that employees are aware of and understand their obligations in relation to the respective policies.

8.0 RECOMMENDATION

8.1 The Resources Committee is asked to approve the appended GMCA information governance policies:

- Appendix 1 - Appropriate Policy (Special Category Data)
- Appendix 2 - Data Subject Rights Policy
- Appendix 3 - Data Quality Policy
- Appendix 4 - Anonymization and Pseudonymization Policy
- Appendix 5 - Freedom of Information and Environmental Information Regulations Policy

Policy: Pseudonymisation and Anonymisation 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

Document Version Control 2
1. Introduction 4
2. Policy Scope 5
3. Policy Statement 5
4. Roles and Responsibilities 6
5. Definitions 9
6. Anonymisation and Psuedonymisation principles 10
7. Anonymisation 11
8. Pseudonymisation 12
10. Legal and Professional Obligations 12
11. Training 13
12. Compliance and Monitoring 13
Appendices 14
Appendix 1: Related Policies and Procedures 14
Appendix 2 Further Information and Guidance 14

1. Introduction

1.1 The Greater Manchester Combined Authority (GMCA) was established in April 2011 and since 2017 also has in place the elected Mayor of Greater Manchester who works collaboratively with other public sector organisations, voluntary and private enterprises in order to drive beneficial outcomes for the GM region and the lives of all its citizens. By encouraging economic growth, facilitating public sector reform, provision of a front-line fire and rescue service, Police and Crime Commissioner functions and delivering the Greater Manchester Strategy.

1.2 In order to fulfil its functions and duties as a Combined Authority the GMCA collects and processes personal data relating to individuals who use the services it provides, past, present and prospective employees, contractors, suppliers, clients, and others with whom it communicates.

1.3 The GMCA is responsible for being instrumental in the strategic changes required across GM to enable increased information sharing across public service delivery for public benefit. It is therefore imperative that organisational compliance with Data Protection laws for the GMCA is one that is continually striving for excellence.

1.4 As a public Authority the GMCA is obliged to comply with the UK General Data Protection Regulation[1] (UK GDPR) and the Data Protection Act 2018[2].Both of these pieces of legislation require the GMCA to process only the minimum amount of personal data needed for one or more specified purposes. Also to not use information that identifies individuals unless necessary.

1.5 The UK GDPR provides a set of principles to follow to handle personal data appropriately and in accordance with the law. The principle that supports the practice of only using the amount of personal data necessary is called the *'Data minimisation principle*' and is set out in Article 5(c) of GDPR. Data minimisation is also formally recognised in the third Caldicott[3] principle in relation to processing patient data and information, and it states: "Don't use personal confidential data unless it is absolutely necessary".

1.6 There are various ways in which data use can be minimized, where personal data isn't necessary for the purposes or the outcomes that are trying to be achieved, and so Pseudonymisation and/or anonymization techniques should be applied to the data.

[1] Guide to the UK General Data Protection Regulation (UK GDPR) | ICO
[2] Data Protection Act 2018 (legislation.gov.uk)
[3] The Caldicott Principles - GOV.UK (www.gov.uk)

1.7 Effective pseudonymisation and/or anonymisation processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality. They are part of the Data Protection by Design[4] approach through which data protection is integrated into processing activities and business practices, from the design stage right through the lifecycle. They will often be relevant to a Data Protection Impact Assessment (DPIA) and form a key technical measure to ensure processing complies with the data protection principles.

1.8 This policy therefore sets out the commitment of how the GMCA will comply with the data minimisation principle and the use of pseudonymisation and anonymisation.

2. Policy Scope

2.1 This policy applies to all personal information including health data, 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 personal information and special category information processed by the GMCA on behalf of other organisations

2.2 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.

2.3 This policy applies to data processing where the GMCA is a data controller in its own right or is a data controller in relation to a multi-agency data sharing partnership. This policy also applies when the GMCA is acting as a Data processor on behalf of one or more data controllers

3. Policy Statement

3.1 This policy states how the GMCA will comply with the GDPR's data minimization principle using anonymisation and pseudonymization techniques

3.2 As the GMCA processes a wide range of information this policy does not provide detailed guidance on the application of anonymisation and pseudonymization techniques or individual areas of application; these will be captured within the supporting procedural documents.

[4] Data protection by design and default | ICO

4. Roles and Responsibilities

4.1 Chief Executive

The Chief Executive is 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 therefore ultimately responsible for ensuring the GMCA only processes personal identifiable data where necessary and complies with data minimization principles.

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 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.

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.
- Acting as the contact point for the supervisory authority (Information Commissioners Office) on all data protection issues, including data breach reporting.

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) are members of the Extended Leadership Team. Their 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 their business area complies with the data minimisation principle
- to consider pseudonymisation and anonymisation techniques at the project initiation stage, as part of the DPIA process

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:

- Ensuring all team members keep their training up-to-date
- Supporting the IAO by ensuring their business area complies with the data minimisation principle and the use of pseudonymisation and anonymisation

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 their business area complies with the data minimisation principle and the use of pseudonymisation and anonymisation techniques to remove personal identifiers from the processing of information where appropriate.

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 the data they're responsible for is anonymized or pseudonymised where it is appropriate to do so.
- Ensuring all breaches or suspected breaches of confidentiality or information security are reported for immediate investigation. In particular, this includes the unauthorised reversal of pseudonymisation.

4.10. All staff must:

- All staff who create, receive and use personal information including health data, special category or criminal conviction data have pseudonymisation and anonymisation responsibilities under the Data Protection Act and supporting information governance policies.
- Follow this policy for all processing of personal data throughout the GMCA.
- Protect any personal data 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 personal 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
- Ensuring all breaches or suspected breaches of confidentiality or information security are reported for immediate investigation. In particular, this includes the unauthorised reversal of pseudonymisation.

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.

5. Definitions

5.1 **Personal Data -** Any information relating to a natural person who can be identified directly from the information or could be in combination with other information.

5.2 **Anonymisation -** The process of turning data into a form which does not identify individuals and where identification is not likely to take place. Anonymisation describes the process of data de-identification, producing de-identified data that cannot be linked to the original source or to an individual**.**

5.3 **Anonymised Data -** Data in a form that does not identify individuals and where identification through its combination with other data is unable to take place.

5.4 **De-identification -** The de-identification of data refers to the process of removing or obscuring any personally identifiable information from records in a way that minimises the risk of unintended disclosure of the identity of individuals and

information about them. Methods used to de-identify information may vary depending on the circumstances but should be appropriate to protect the confidentiality of the individuals and the intended secondary use of the data.

5.5 **Pseudonymisation -** This is a method of removing the identifiable nature of data by using a unique identifier which does not reveal their 'real world' identity. In order to de-identify the data a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without the individual being identified. The ICO draws a distinction between anonymisation techniques used to produce aggregated information and those such as pseudonymisation that produce anonymised data but on an individual-level basis.

Data Protection legislation supports the use of pseudonymisation as an appropriate safeguard where anonymisation is not practical, yet it should be recognised that data that has undergone pseudonymisation can still be considered information about an identifiable natural person.

5.6 **Pseudonym -** This is a coded reference used to conceal/de-identify the personal data. This reference can be stored securely in order to re-identify the data back to its original form if necessary.

5.7 **Aggregation –** The merging of data to present figures in a way which does not allow the identification of individuals. This is where data are displayed as totals, so no data relating to or identifying any individual is shown. Small numbers in totals are often suppressed through 'blurring' or by being omitted altogether. Consolidating

6. Anonymisation and Pseudonymisation principles

6.1 Data Protection legislation classifies pseudonymised data as personal data and therefore must be processed in accordance with all data protection legislation. If the GMCA has access to the pseudonymised data and the identifiable personal confidential data; the key to the pseudonym; or has the means to re-identify pseudonymised data, the pseudonymised data remain in scope for full compliance with data protection legislation.

6.2 Data protection legislation states that data which is truly anonymised in such a way that individuals cannot be identified or re identified does not fall within the scope of the UK GDPR and therefore does not fall within the scope of the Data Protection Act either.

6.3 It is always preferable to fully anonymise any data that has the potential to reveal something personal about an individual, either from that data alone or when combined with other data.

6.4 Where data cannot be used in an anonymised format, due to the need to link datasets, because data may ultimately need to be re-identified or processed in identifiable format, the personal or data or pseudonymised data may be used

provided there are strict controls in place to prevent unauthorised access and unauthorised re-identification.

6.5 The key advantages of using anonymised data as opposed to identifiable data include:

- it is easier to use anonymised data in new and different ways because the data protection legislation “purpose limitation rules do not apply;
- protection against unauthorised access or disclosure of personal data; fewer legal restrictions apply;
- allow for the sharing of data with colleagues and teams for analysis
- allows organisations to make information public while still complying with their data protection obligations; and
- the disclosure of anonymised data is not a disclosure of personal data.

6.6 The GMCA will carry out a thorough risk analysis on the likelihood and potential consequences of re-identification at the initial stage of producing and disclosing anonymised or pseudonymised data. The GMCA will always use a DPIA (Data Protection Impact Assessment) to undertake this assessment of risk, in line with Article 35 of GDPR.

6.7 The risk of re-identification will differ according to the way the anonymised or pseudonymised information is disclosed, shared or published. Publication to the wider public would be considered far more risky than limited access.

6.8 Any pseudonymization and anonymisation techniques used in GMCA projects must therefore be employed as part of a ‘holistic methodology’ of technical and non-technical processes to protect personal data enshrined in the concept of privacy by design and default (Article 25).

7. Anonymisation

7.1 The organisation will use de-identification and anonymisation techniques to obscure or remove the identifiable data items within a person’s records sufficiently that the risk of potential identification of the subject or a person’s record is minimised to acceptable levels, so as to provide effective anonymisation, where appropriate. Recital 26 of GDPR defines anonymous information, as "…information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". The GDPR does not apply to anonymised information as set out above in Section 6.

7.2 Anonymised data will allow information which originated as personal confidential data to be available in a form that is rich and usable, whilst protecting the confidentiality of the individual.

7.3 The organisation will continue to comply with role-based access controls when using de-identified and anonymised data.

The organisation will achieve de-identification and anonymisation by:

- Removing personal identifiers (e.g. name, date of birth, physical description etc)
- The use of identifier ranges, for example; value ranges instead of age.
- Aggregation.
- Using a pseudonym (although, as covered further below, pseudonymising data will not necessarily completely ensure that re-identification is impossible).

The organisation will ensure that any commissioning and contracting on behalf of the GMCA will include assurances that the Provider's processes are robust in respect of the supply of data and data minimization principles.

The most up to date guidance from the Information Commissioners Office on Anonymisation can be viewed here; https://ico.org.uk/media/1061/anonymisation-code.pdf

8. Pseudonymisation

8.1 Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable human being. Essentially this means substituting the identifiable part of the data with something else, in a way that the data can only be re-identified using a key for example.

The GMCA will effectively pseudonymise data by:

- Removing personal identifiers and ensuring Personal Identifiable Data is replaced with a unique pseudonym;
- When using pseudonymisation externally, it's important to use different pseudonyms internally, such that internal data use/processes are not compromised;
- Pseudonymised data will have the same security applied to it as all other Personal Identifiable Data

10. Legal and Professional Obligations

10.1 The GMCA will take actions to comply with the relevant legal and professional obligations, in particular:

- General Data Protection Regulation and Data Protection Act 2018

- Human Rights Act 1998
- Common Law Duty of Confidentiality
- The Information Commissioner's Office (ICO) code: anonymisation: managing data protection risk code of practice
- NHS Digital Data Security and Protection Toolkit

11. Training

11.1 The GMCA will provide relevant training both on line and face to face to ensure that staff understand the legislation and its application to their role.

11.2 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 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 personal information. Failure to do so may result in disciplinary action and legal prosecution.

12.2 If an employee is in any doubt about how to handle personal information or to apply the pseudonymisation/anonymisation techniques mentioned above, they should speak to their line manager or contact the Information Governance Team OfficeofDPO@greatermanchester-ca.gov.uk

12.3 This policy will be reviewed at regularly by the Information Governance Team to ensure that it is updated in line with any change in legislation.

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

Appendices

Appendix 1: Related Policies and Procedures

- GMCA Information Disclosure Policy.
- GMCA Information Security Policy
- GMCA Records Retention Policy
- GMCA Data Quality Policy
- GMCA Subject Access Policy
- GMCA Disciplinary Policy
- GMCA Employee Code of Conduct
- GMCA Freedom of Information Act Policy

Appendix 2 Further Information and Guidance

Data Protection Officer

Data Protection Officer – Assistant Director Information Governance

GMCA, Churchgate House, 10, Oxford Street, Manchester M16EU

Email: OfficeofDPO@greatermanchester-ca.gov.uk

Information Commissioner

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Tel: 0303 123 1113

www.ico.org.uk

On line Resources

- ICO – www.ico.org.uk
- GMCA intranet

GMCA GREATER MANCHESTER COMBINED AUTHORITY

Resources Committee

Date: 30 July 2021

Subject: Core Investment Team

Report of: Eamonn Boylan, Chief Executive

PURPOSE OF REPORT:

This report relates to proposals within the Greater Manchester (GM) Core Investment Team to create extra posts, further to the report to the GMCA in June 2021. The proposed changes are fully funded by the Team's budget. These roles have been identified to support the Local Authorities to bring forward their development plans and more efficiently manage the central government funding that has been awarded to GM through the Getting Building Fund and Brownfield Housing Fund.

RECOMMENDATIONS:

The Resources Committee is requested to approve the amendment of the structure as follows:

1. Creation of 1 Senior Transaction Manager Post – new role
2. Deletion of 1 Transaction Manager Post
3. Creation of 1 Investment Transaction Manager Post – new role but based on existing Transaction Manager level
4. Creation of 1 Quantity Surveyor Post (Grade 11) – additional role but based on existing Grade 11 within the service.

CONTACT OFFICERS:

Name: Andrew McIntosh
Position: Director of Place
E-mail: andrew.mcintosh@greatermanchester-ca.gov.uk

Name: Laura Blakey
Position: Investment Director
Email: laura.blakey@greatermanchester-ca.gov.uk

Equalities Impact, Carbon and Sustainability Assessment:

Impacts Questionnaire

Impact Indicator	Result	Justification/Mitigation	Guidance
Equality and Inclusion			***See Equalities Impact Assessment Result***
Health			
Resilience and Adaptation			
Housing			
Economy			
Mobility and Connectivity			
Carbon, Nature and Environment			***See Carbon Assessment Result***
Consumption and Production			

Risk Management:

N/a

Legal Considerations:

N/a

Financial Consequences – Revenue:

The Core Investment Team is fully funded by interest and arrangement fees earned on housing and commercial property loans. The Senior Transaction Manager post will be funded through commercial property income and the remaining loans through Housing Investment Fund loan surpluses, as approved by the GMCA in June 2021.

Financial Consequences – Capital:

There are no capital financial consequences

Number of attachments to the report: 1

Comments/recommendations from Overview & Scrutiny Committee

BACKGROUND PAPERS:

- Report to the GMCA in June 2021: Utilisation of GM Housing Investment Loans Fund and Evergreen Fund surpluses and Inclusion of Brownfield Housing Fund Site

TRACKING/PROCESS	
Does this report relate to a major strategic decision, as set out in the GMCA Constitution?	No
EXEMPTION FROM CALL IN	
Are there any aspects in this report which means it should be considered to be exempt from call in by the relevant Scrutiny Committee on the grounds of urgency?	
GM Transport Committee	
Overview & Scrutiny Committee	

1. INTRODUCTION/BACKGROUND

1.1 In order to successfully meet future housing need in Greater Manchester, GMCA recognises the need to increase and accelerate housing delivery across the city region. The GMCA has launched the Housing Vision which sets out Greater Manchester's vision for the type and mix of development it would like to see brought forward across GM. The GM Housing Strategy has been published and provides the policy context. These documents set out the preference to deliver brownfield sites across GM, the desire to deliver a greater number of social and affordable houses and to support SME house builders and Community Led Housing initiatives. The GMSF (and emerging Places for Everyone document) includes a GM target delivery of 50,000 new affordable houses across GM over the period of 2018-2037.

1.2 In December 2018, the Combined Authority approved that the majority of GM Housing Investment Loan Fund (GMHILF) surpluses would be ring-fenced to support affordable housing priorities as identified in the GM Housing Strategy.

1.3 Given the current pressures across the Local Authorities it is proposed that a number of additional roles are created within the Core Investment Team that can provide specialist investment support to the Local Authorities to meet the objectives set out within the Housing Strategy.

1.4 It is also proposed that a Senior Transaction Manager post be created within the Core Investment Team to support the Investment Director in their additional responsibilities following the appointment of the second Investment Director to the Director of Place role.

2. ROLES TO BE CREATED

2.1 The are several roles that have been identified to be created to support the Local Authorities bring forward their development plans and more efficiently manage the central government funding that has been awarded to GM through the Getting Building Fund and Brownfield Housing Fund. This paper seeks approval to those roles. The roles will sit within the Core Investment Team to ensure that the investment skill set continues to be centralised in one team and allow for a blend of work across the Team. The posts can be summarised as follows:

a. **Senior Transaction Manager (Salary: £75-80k dependent on the candidate)** – to support the Investment Director in their additional responsibilities. The Investment Director has overall day to day responsibility for the GMCA's investment funds, of which circa £300m is under direct management. The role profile for the Senior Transaction Manager is to be developed but will encompass the responsibilities of a Transaction Manager role (as set out in the Appendix) plus additional line manager, budget and deputy responsibilities.

b. **Investment Transaction Manager** - to support the development of robust investment proposals (Local Investment Frameworks) across the GM Growth Locations. The Transaction Manager role is a generic role (with this role having a district focus) within the team and the role profile is attached as an Appendix.

c. **Quantity Surveyor** - to provide an in-house Monitoring Surveyor Role for existing grant programmes. The Quantity Surveyor is a generic role within the team and the role profile is attached as an Appendix.

The salary levels for these roles are consistent with existing roles within the team. The Investment Transaction Manager is on equivalent level to existing Transaction Manager roles (£69,485) and the Quantity Surveyor is on par with the existing role within the service (Grade 11 £52,076 - £56,676).

The Senior Transaction Manager, who will act as a deputy and support to the Investment Director, is paid at a level set midway between Transaction Manager and Investment Director. This is felt to be commensurate with their responsibilities which will include line management of Transaction Managers.

Whilst the creation of an additional Grade 11 role does not require approval from Resources Committee it has been included for completeness.

4. RECOMMENDATIONS

4.1 Recommendations are set out at the front of this report.

5. CONCLUSION

5.1 The proposals within this report set out the requirements for additional resource into the Core Investment Team in order to provide the capacity for additional specialist investment support to be provided to Local Authorities.

Appendix

Transaction Manager Role Profile

The Core Investment Team is responsible for managing funding provided through the GM Investment Framework and the GM Housing Fund in support of the economic growth of the region. The team supports the development of business cases for investment and develops a pipeline of future projects to support the regeneration of region.

Key Role Descriptors:

This role is a senior post within the Core Investment Team to support the operation of the funds under management. The roleholder will be responsible for developing and managing a portfolio of loan and equity investments in private-sector led business and property development schemes across Greater Manchester, in line with an agreed Investment Strategy and Risk Management Framework.

Key Role Accountabilities:

Ensure that resources are commissioned and co-ordinated in a well-planned and controlled manner, ensuring that requirements and resource levels are fully identified.

Ensure effective communication through high quality reports, informal briefings and presentations to GMCA governance bodies, elected Members, MPs and organisations from the public, private and voluntary sectors.

Ensure that GMCA corporate requirements are consistently met, including for business planning, performance management and budget monitoring.

Specific Role Accountabilities:

Develop and manage a portfolio of loan and equity investments in private-sector led businesses and property development schemes across Greater Manchester, in line with an agreed Investment Strategy and Risk Management Framework, preparing detailed analysis to illustrate sensitivities and options in order to negotiate robust funding structures.

Report to the GMCA Investment Committees on investment propositions and pricing, identifying risks and mitigation strategies, and monitor the performance of investments made by the Funds to ensure that GMCA funding is safeguarded.

Establish good working relationships with a range of key partners including property developers, businesses, professionals and investors, and senior officers within Greater Manchester's constituent local authorities.

Instruct and manage external financial, property, construction and legal advisors to support due diligence, loan facility development, contracting and monitoring of investments.

Support the development of operational processes and credit and risk management practices.

Demonstrate personal commitment to continuous self development and service improvement.

Through personal example, open commitment and clear action, ensure diversity is positively valued, resulting in equal access and treatment in employment, service delivery and communications.

Where the roleholder is disabled every effort will be made to supply all necessary aids, adaptations or equipment to allow them to carry out all the duties of the role. If, however, a certain task proves to be unachievable, job redesign will be given full consideration.

Transaction Manager – Key Competencies and Technical Requirements

Behavioural Competencies

- **Leadership & Management:** The behaviours and actions of our managers define how we work and what we achieve.
- **Change:** Improving services and making the most of resources.
- **Delivery:** Delivery of high quality services is an essential part of what we do.
- **Influence:** Effective relationships give the best results.

Generic Skills

- **Communication:** Is able to effectively transfer key and complex information to all levels of staff, adapting the style of communication as necessary and ensuring that this information is understood.
- **Analytical:** Application of strong analytical reasoning skills and intellectual focus, taking in the wider external and internal environments. Proactively think through problems rather than reactively following a procedure-driven approach.
- **Commercial:** Demonstrates sound business intelligence and ability to identify commercially viable opportunities and secure value for money in service delivery.
- **Problem Solving and Decision Making:** Ability to react to immediate problems of a highly complex nature with associated risk factors and deliver pragmatic solutions sometimes under extreme pressure.
- **Financial Management:** Ability to represent the organisation at a senior level in financial, commercial and general management relationships with other organisations in both public and private sectors.
- **Project Management:** Ability to identify, assess and respond to the key risks to the achievement of strategic and operational objectives.
- **Strategic:** Thinks and acts cross-functionally and cross-organisationally, beyond one's own professional areas of specialism, perceiving the wider picture and the implications of short-term decisions for the achievement of long-term strategic goals.

Technical requirements (Role Specific)

Qualifications

- Degree level qualification (essential)
- Relevant professional qualification, e.g. Chartered Accountant

Experience

- Experience with an organisation involved in the funding of, or accessing funding for businesses and/or property/housing development schemes;

- Direct experience of scoping, structuring and monitoring funding (including recoverable investment) for businesses and/or property/housing development schemes;

- Specification, interpretation and constructive challenging of construction, property market, valuation, financial and legal advice;

- Negotiation with funding recipients, funding partners and key stakeholders;

Quantity Surveyor – Role Profile

JOB PURPOSE

The Core Investment Team oversees the investment of over £600m of funding into businesses and property developments, alongside providing commercial finance support to the wider CA. Of the £600m, circa £400m is directly invested and monitored by the Team.

The Quantity Surveyor is responsible for all property monitoring, ensuring that projects are running to budget and highlighting development issues. This is a technical role requiring strong property knowledge and experience.

KEY RELATIONSHIPS

- Developers
- Monitoring Surveyors
- Lawyers
- Local Authorities
- Colleges/Universities
- Transaction Managers
- Investment Directors

KEY RESPONSIBILITIES

- Overall responsibility for all property monitoring (circa £400m), including skills capital project monitoring.
- Attend site visits for all large and/or complex property schemes to understand the developments' progress and provide challenge when required.
- Review all external Monitoring Surveyors reports to identify key risks/issues.
- Advise the Transaction Manager on solutions to risks/issues that have been identified and support the conversations with the Developers around these issues.
- Prepare drawdown reports summarising the status of the development highlighting any significant risks and mitigating factors.
- Liaise with Local Authorities to understand their development pipelines.
- Advise the Transaction Managers on issues identified in the Construction reports, liaising with the lawyers when relevant.
- Line manage the Junior Quantity Surveyor with responsibility for overseeing their work.

General

- People management
- Writing reports

NB: This list of duties and responsibilities is by no means exhaustive, and the post holder may be required to undertake other relevant and appropriate duties as required.

KNOWLEDGE, SKILLS AND EXPERIENCE

Knowledge & Experience

- Chartered Quantity Surveyor with full RICS membership – MRICS (or equivalent)
- Ideally have minimum [3/5] years PQ experience
- Previous Residential/Commercial/Education project experience will be looked upon favourably
- Demonstrate good working knowledge of the JCT/NEC suite of contracts
- Understanding of property lending and structuring of transactions
- Ability to lead from the front as regards to client facing meetings, dealing with multi-disciplined teams and project delivery
- Experience of line management responsibilities

Skills & Behaviours

- Must be able to handle multiple jobs and manage their own workload, ensuring all deadlines are met.
- The role requires direct liaison with clients, developers and their professional teams and as such, excellent inter-personal skills are key.
- Confident and concise communicator both verbally and in writing.
- Accurate and excellent attention to detail.
- Pro-active and enjoys working autonomously and as part of a wider team.
- Ability to coach and mentor team members.
- Must have proficient IT skills, particularly MS Office (Word, Excel, PowerPoint).
- A collaborative approach to work, willing to share knowledge, experience, ideas and expertise for the betterment of group and self.
- Ability to work flexibly and creatively as part of an effective team
- Commitment to high standards of customer care and public service
- Requirement to travel outside the county to attend meetings etc. when required may include overnight stay
- Occasional requirement to attend residential training courses
- To be willing to work flexibly as occasional evening and weekend working may be required
- Willingness and ability to travel across the county when required, within a reasonable time to meet the role demands (individuals providing their own vehicle for use will be eligible for casual car user rate.

This page is intentionally left blank