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Superseded Documents:	**Cross Reference – Related policies and procedures:**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 It supersedes any previous versions of this document, which are now withdrawn.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

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