Transport for Greater Manchester

Transport for Greater Manchester Policy

Data Protection Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	01 September 2020	Document Reference no.	Data Protection Policy
Version No.	1.0	Prepared by:	Senior Information Governance Lead/Deputy Data Protection Officer.
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim **Date: 30/09/2020**		Full Impact Assessment completed: ~~YES~~/NO Not required **Validated by Equality Officer signature:** **Date: 30/09/2020**
Authorisation Level required:	Performance Board		Staff Applicable to: All Staff, contractors, agency staff, volunteers
Authorised by: Date:	Performance Board Data Protection Officer Head of Legal/Senior Information Risk Owner October 2020		Implementation date: October 2020 Annual review date: October 2021

Contents

1. Introduction

1.1 Data Protection legislation has existed in the UK for over 4 decades, over the past few years there has been an unprecedented amount of work undertaken to develop data protection laws that provide the right level of protection for individuals privacy in the current and evolving digital era. From May 2018 all organisations in the UK were obligated to comply with the General Data Protection Regulation and the Data Protection Act 2018.

Data Protection laws provide the legal framework within which organisations that process personal data can do so applying the appropriate protection to individual's privacy rights.

1.2 In the UK the protection of personal data is governed by the Data Protection Act 2018 (DPA 2018) which is the UK's implementation of the General Data Protection Regulation (GDPR). In addition, Article 8 of the Human Rights Act 1998 gives broader protection by affording everyone the right to respect for their private and family life, home, and correspondence.

1.3 Transport for Greater Manchester (TfGM) is required to comply with the Data Protection legislation and to demonstrate how it does so, along with ensuring that it has embedded the concept of Privacy by Design into its processes, Privacy by Default into the design of its systems and has put appropriate mechanisms in place to protect personal data.

1.4 Transport for Greater Manchester was established in April 2011 and is responsible for delivering the Greater Manchester Transport Strategy and delivering transport policies set by the elected Mayor of Greater Manchester, the Greater Manchester Combined Authority (GMCA) and Greater Manchester Transport Committee.

1.5 In 2017 the GMCA launched TFGM's Transport Strategy 2040 which sets out the long-term vision and approach to planning GM transport needs and aspirations. The vision for Greater Manchester to have ***'World class connections that support long-term, sustainable economic growth and access to opportunity for all'***, and the four key elements that underpin this:

- Supporting sustainable economic growth;
- Protecting our environment;
- Improving quality of life for all; and
- Developing an innovative city-region.

1.6 TfGM work collaboratively with partners across the GM family of organisations including the Greater Manchester Combined Authority (GMCA), Local Authorities, other public

sector organisations, Not for Profit and private enterprises in order to help in improving the lives of all its citizens, by encouraging economic growth, facilitating public sector reform and delivering the Greater Manchester Strategy.

1.7 TFGM's remit across Greater Manchester includes:

- Working closely with bus, tram and train operators to help improve the full journey experience.
- Owning Metrolink – the UK's largest light rail network –expanding the network and planning for its future.
- Promoting and investing in walking and cycling (including electric scooters) as safe, healthy and sustainable ways to travel.
- Paying for bus services at times and in areas where no commercial bus services are provided.
- Keeping traffic flowing on some of Greater Manchester's busiest roads by managing a 360 mile 'Key Route Network'.
- Owning Greater Manchester's bus stations, stops and shelters and investing in new, modern transport interchanges.
- Subsidising more affordable fares to help older people, children and disabled people get around.
- Developing easier, smarter ways to travel and planning journeys by using data and technology.
- Playing a leading role in coordinating Greater Manchester's plans to reduce transport-related air pollution.
- Preparing an assessment around Bus Reform.

1.8 In order to fulfil its functions and duties TfGM collects and processes personal data and special category data relating to customers who use the services it provides, members of the public, past, present and prospective employees, contractors, suppliers, clients, strategic partners and others with whom it communicates and needs to share data.

1.9 TfGM collects and processes personal data for the day to day running of the organisation but also to fulfil its wider role in delivering the Transport Strategy 2040. It is therefore imperative that organisational compliance with Data Protection laws is one that is continually striving for excellence.

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

1.11 Any breach of this policy will be investigated and may result in disciplinary action and/or 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 TfGM 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 TfGM 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 TfGM employees, seconded staff members, volunteers, third party contractors, temporary staff and employees of other organisations who directly or indirectly support TfGM services. This policy applies to all TfGM functions and those of its subsidiary companies.

2.4 This policy should be read together with the "appropriate policy document" for TfGM that sets out how special category and criminal convictions personal data will be protected in line with Schedule 1 of the DPA 2018.

2.5 This policy applies to data processing where the TfGM 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 TfGM is acting as a Data Processor on behalf of one or more data controllers.

3 Policy Statement

3.1 Data Protection legislation provides a legal framework within which TfGM 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, subsidiary companies, suppliers, law enforcement and other partner agencies.

3.2 This policy sets out how TfGM will comply with Data Protection legislation to ensure that all the personal data held is collected, stored, and used lawfully and fairly with the right level of protection applied to it.

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 Chief Executive's liability with regards to offences committed under the Act. This places responsibility right at the highest level of seniority and leadership of the organisation.

4.2 Senior Information Risk Owner (SIRO)

The SIRO has an overall strategic responsibility for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers. The SIRO is responsible for:

- Acting as an advocate for managing information risk within TfGM.
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners
- Providing written advice to the Accounting Officer on the content of their annual governance statement regarding information risk.
- Owning the organisation's information incident management framework.

The SIRO is the Head of Legal Services who is also Legal Counsel for TFGM.

4.3 Data Protection Officer (DPO)

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

- Informing and advising TfGM 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).

TfGM will meet 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 the organisation, i.e. board level at the TfGM - this is the SIRO;
- the DPO operates independently and cannot be 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;
- the DPO has appropriate access to other services within the organisation so that they can receive essential support, input or information.

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

4.4 Deputy Data Protection Officer

TfGM also has a Deputy DPO who deputises for the DPO when the DPO is unable to fulfil their duties and supports the DPO in provision of the DPO function responsible for day-to-day matters relating to data protection compliance and a point of contact for data protection issues. The Deputy DPO is employed by GMCA but on full time secondment to TfGM.

4.5 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) within TfGM are the Functional Leads who are also members of the TfGM Information Governance Board. 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 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 a Record of Processing Activity.
- Management of Information Asset Register (IAR) and Record of Processing Activity (ROPA).
- 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 TfGM Information Security and associated policies and procedures to reflect local and national standards and guidance and legislative requirements. They also support TfGM in ensuring compliance with information security requirements. This role reports to Head of IS Operations.

4.8 Heads of Department/Functional Leads 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 any changes to existing processing and changes to legislation.
- 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 TfGM's mandatory data protection training every year.

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 TfGM's mandatory data protection training every year.

4.10. All staff must:

- Follow this policy for all processing of personal data throughout TfGM
- 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 TFGM Incident procedure.
- Keep up to date with all Data Protection and Information Governance training that is appropriate to their role.

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 TfGM policies and procedures.
- Manage and monitor any Information Security Breaches in line with the TfGM Information Security Breach Policy.
- Develop and deliver training as required.

5. Principles

5.1 Under Data Protection Act 2018 there are six data protection principles plus the Accountability principle which TfGM must comply with.

Lawfulness, Fairness and Transparency.

Any processing of personal data must be done lawfully and fairly and without adversely affecting the rights of the individual. Therefore, the TfGM must have a lawful basis in order to process personal information and must explain this to the data subject along with the purpose of the processing and the identity of anyone to whom data maybe disclosed or transferred.

TfGM will only handle personal data in ways that people would reasonably expect and will not use it in ways that have unjustified adverse effects on them. In order to ensure that any personal data processing is fair the TfGM will undertake Data Protection Impact Assessments or Personal Data Processing Assessment (PDPA) prior to any processing commencing.

TfGM will be clear, open and honest with individuals from the start about how it will use their personal data. They will make available detailed privacy notice/s for data subjects so that they are provided will full transparency about the processing of their data.

Purpose Limitation

Personal information must only be collected for a specific legitimate purpose and processed in accordance with this purpose. It must not normally be collected for one purpose and used for another purpose unless it is compatible with the original purpose

for which it was collected i.e. any additional purpose must directly relate to the original purpose.

Before any collection or processing of personal information occurs, TfGM will define a precise purpose for the processing. This purpose will inform the legal basis for the processing and form the foundation of the necessary privacy notice/s to be made available to the data subject. The purpose will be agreed by all parties involved in the processing.

TfGM will only collect personal data for specified, explicit and legitimate purposes, and will inform data subjects what those purposes are in a privacy notice when the data is first collected.

TfGM will not use personal data for purposes that are incompatible with the purposes for which it was collected. If personal data is to be used for a new purpose that is compatible, TfGM will inform the data subject first.

Where the data processing is undertaken within multi-agency data sharing initiatives to which TfGM is party, then TfGM will work together with the partners to develop common purposes for the processing and common privacy or transparency notices.

Further processing of personal data for archiving in the public interest, scientific or historical research purposes or statistical purposes are not considered incompatible with the initial purposes.

Data Minimisation

This considers personal data processed for a purpose should be adequate, relevant, and limited to what is necessary for the stated purpose/s.

When processing personal data, care should be taken only to process what is needed to fulfil the purpose notified to the data subject. Each circumstance will be different and so it is important to justify why it is necessary to collect/process the data for the intended purpose. It is not justifiable to collect/process data 'just in case'.

For special category data or criminal offence data, it is particularly important to make sure only the minimum amount of information is collected and retained.

TfGM will ensure that it only collects the minimum personal data needed for the purpose for which it is collected and that the data collected is adequate and relevant and will use data protection impact assessments to do this and to ensure the data collected is not

excessive. Where applicable TfGM will use national guidance and relevant legislation to determine information that should be collected.

Where the data processing is undertaken within multi-agency data sharing initiatives to which TfGM is party, then TfGM will work together with the partners to undertake a Data Protection Impact Assessment (if appropriate) to determine the minimum personal data needed.

Accuracy

Data should be accurate and, where necessary, kept up-to-date TfGM operate a data accuracy policy and processes and procedures to support this.

TfGM will take all reasonable steps to ensure that any personal data it processes is accurate and kept up to date.

Where it is found that any data held is inaccurate the error will be rectified straight away. Any other organisation/individual to whom the inaccurate data has been disclosed must also be notified of the error immediately.

TfGM will ensure that relevant communication opportunities and design of systems enables the timely identification and rectification of inaccurate data.

Where the data processing is undertaken within multi-agency data sharing initiatives to which the TfGM is party, then TfGM will work together with the partners to agree the processes for checking data accuracy that are to be used.

Storage Limitation

Personal data should not be kept longer that is necessary for the purpose.

TfGM will take all reasonable steps to erase or permanently anonymise any personal data that is no longer required.

TfGM operate a records retention policy which that sets out the timescales for retaining different record types and the methods to be applied to ensure data is disposed securely and safely.

The period for which the personal data will be stored, or the criteria used to determine that period will be documented in TfGM's privacy information provided to data subjects.

Where the TfGM shares personal data with other organisations, they will agree the retention and destruction processes between with the partners to set out what happens once there is no longer a need to share the data.

It should be noted that it is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data.

Integrity, Confidentiality and Availability (Security)

Information security is important, as it is an essential line of defence in keeping data safe, secure, and available for use to support critical business delivery.

This security principle states that TfGM will ensure the appropriate level of security. In assessing the level TfGM will demonstrate is has considered levels of security in all areas of personal data processing. TfGM will also consider this in relation to the state-of-the-art technology and costs of implementation, as well as the nature, scope, context, and purpose of the processing

Organisations are required to have a level of security that is 'appropriate' to the risks presented by the processing.

TfGM will ensure that security measures appropriate to the identified risks are in place to protect against any accidental loss, destruction, theft, or damage and any unlawful or unauthorised processing of personal data. Where appropriate and required data minimisation, anonymisation or pseudonymisation will be used to reduce the risk of sensitive data being compromised. TfGM operates a policy which covers data minimisation

TfGM will operate a robust Information Management procedure that will ensure all security breaches of personal and special category data are dealt with in a timely manner, minimising any impact to those affected.

Where TfGM has contracted with a third party to process data on their behalf, appropriate Data Processing Contracts must be put in place. These contracts must contain a number of specific conditions as set out in legislation which include:

- The processor must only act on the written instruction of the data controller.
- The processor must take appropriate measures to keep the personal data secure.

Accountability

Accountability is a data protection principle and requires organisations to ensure that all the data protection principles are adhered to and to be able to demonstrate compliance with all the principles.

Measures that must be taken to demonstrate compliance include:

- Implementing appropriate security measures.
- Ensuring records are kept of all personal data 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.
- Ensuring that a Data Protection Officer is appointed to provide independent advice and monitoring of the departments' personal data handling, and that this person has access to report to the highest management level of the department.
- Having written contracts in place with data processors.
- Having in place internal processes, policies, and procedures to ensure that personal data is only collected, used, or handled in a way that is compliant with data protection law.
- Recording and, where necessary, reporting personal data breaches.
- Adhering to relevant codes of conduct and signing up to certification schemes.
- Implementing measures that meet the principles of data protection by design and data protection by default. Measures include:
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
- Creating and improving security features on an ongoing basis.

6. Lawful basis for processing

6.1 When processing personal data there must be a valid lawful basis for the processing. There are six lawful basis for general processing of personal data these are:

- Consent: the individual has given clear consent for processing their personal data for a specific purpose.
- Contract: the processing is necessary for a contract TfGM has with the individual.
- Legal obligation: the processing is necessary for TfGM to comply with the law.
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for TfGM to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

- Legitimate interests: the processing is necessary for legitimate interests pursued by TfGM (and is not part of TfGM's "public task") or the legitimate interests of someone else unless there is a good reason to protect an individual's personal information.

6.2 It is the responsibility of TfGM to demonstrate which lawful basis applies to the processing purpose. Therefore, a record must be kept of which basis is being relied on for each purpose and a justification as to why it applies. This helps demonstrate compliance with accountability obligations and will also assist when developing privacy notices.

6.3 Much of the general processing undertaken by TfGM is likely to fall under the public task lawful basis. It should be noted that a public authority cannot use the legitimate interest lawful basis for carrying out its public task.

6.4 In order to use the public task lawful basis, the relevant tasks or authority must be laid down in law. As a Public Body, TfGM has a number of legal duties, functions and delegated powers in order to carry out its functions, which provide the legal basis for the use of personal information.

Listed below is some of the legislation that detail the duties and powers of the TfGM.

- Accounts and Audit Regulations 2015
- Bus Services Act 2017
- Civil Contingencies Act 2004
- Companies Act 2006
- Crime and Disorder Act 1998
- Digital Economy Act 2017
- Environment Act 1995
- Environmental Protection Act 1990
- Equality Act 2010
- Greater Manchester Combined Authority Order 2011
- Health and Safety at Work Act 1974
- Land Compensation Act 1973
- Localism Act 2011
- Local Democracy, Economic Development and Construction Act 2009
- Local Government Act 1972
- Local Transport Act 1968
- Road Traffic Act 1988
- Traffic Management Act 2004
- Transport Act 1968

- Transport Act 1985
- Transport Act 2000Transport and Works Act 1992
- Transport for Greater Manchester (Light Rapid Transit System) (Miscellaneous Provisions) Order 2013.

6.5 When deciding on the legal basis for processing information, TfGM will fulfil its obligations by detailing the specific part of the legislation, the purpose of the processing, and how the legislation applies to the purpose of the processing must be provided by way of a privacy or transparency notice. This notice must also describe any sharing of personal data with other organisations.

6.6 If special category data or criminal conviction data is being processed then both a lawful basis for general processing will be identified along with a condition from GDPR Article 9/ DPA 2018 Schedule 1. There are also additional safeguards that will be put in place including operating an appropriate policy document which explains the controller's procedures for securing compliance with the data protection principles and explains the retention and erasure of personal data.

6.7 Personal data relating to criminal offences and/or convictions are not considered special category data per se, however similar safeguards apply to its processing. As such this data can only be processed in an official capacity, or with specific legal authorisation. This means to process such data, a condition in Schedule 1 of the DPA 2018 must be met along with compliance with the additional safeguards set out in Part 3 of the Act.

6.8 Before any processing of special category or criminal conviction data takes place, the Data Protection Officer should be consulted.

7. Information Sharing

7.1 Government policy places a strong emphasis on the need to share information across organisational and regional boundaries, in order to ensure effective co-ordination and integration of services. The sharing of personal information is fundamental to the work of the TfGM in delivering effective and beneficial services.

7.2 Where the TfGM is involved in the sharing of personal information it will ensure it meets it privacy obligations by implementing best practice and guidance set out in the ICO's code of practice for information sharing.

7.3 The details of information sharing arrangements will be captured in Information Sharing Agreements.

7.4 Where appropriate all information sharing agreements will be captured, held and stored in the Information Sharing Gateway, a process controlled by the TfGM Information Governance Team.

7.5 Information Asset Owners will be responsible overseeing information sharing agreements and adherence with the Information Sharing policy.

7.6 The TfGM when engaging in information sharing will ensure that a DPIA is undertaken to capture that:

- It identifies and articulates the purpose and benefits of the sharing.
- It assesses the necessity and proportionality of the information being shared between partners.
- It identifies the legal gateways the GMCA is relying upon to share the information.
- It identifies and maps all the data flows.
- It provides a level of granularity that allows for all Information Governance and privacy mechanisms to be implemented e.g. privacy notices.
- It identifies all conditions for processing being relied upon through the data flow life cycle.
- The public are consulted when deemed necessary.

7.7 Any risks to privacy identified will be brought to the attention of the DPO.

7.8 TfGM will ensure that any risks which cannot be mitigated sufficiently will be highlighted to the ICO via the DPO and to TfGM's SIRO.

8. Data Subjects Rights

8.1 The Data Protection Legislation gives individuals the following rights over their information regarding their personal information.

- The right to be informed about the use of their information.
- The right of access to their personal information (subject access).
- The right to rectification i.e. the right to require TfGM to correct any inaccurate data.
- The right to request erasure of their personal data.
- The right to restrict processing of their data.

- The right to data portability.
- The right to object to the processing their personal data.
- Rights in relation to automated decision making and profiling.

8.2 Not all these rights are absolute, and some may only apply under certain circumstances. TfGM will publish information on the website about these rights and how these can be exercised.

8.3 Any request from a data subject to exercise their rights must be responded to within strict timescales. Therefore, all request from data subjects wishing to exercise their rights should be forwarded immediately to data.protection@tfgm.com

9. Subject Access Requests

9.1 Any 'data subject' has a right to request access to the information TfGM holds about them. A request does not have to be in writing. TfGM has one calendar month to provide the requested information or enter into discussion with the data subject about extending the time allowed.

9.2 TfGM has Subject Access Request and Data Protection procedures for handling subject access requests and this information is available on the website

9.3 If staff however received any requests these should be immediately forwarded to the Information Governance team - data.protection@tfgm.com

9.4 It should be noted that it is an offence for the data controller or one of their employees to deliberately alter, deface, block, erase, destroy or conceal information to prevent disclosure of any information the data subject would be entitled to receive.

10. Privacy Notices (Transparency notice)

10.1 Data subjects have a right to be informed about the collection and use of their data.

10.2 To that end TfGM will be clear and transparent about how they are using personal information. This will be communicated to the public using Privacy Notices. Any privacy notice produced by TfGM will be concise, transparent, intelligible, easily accessible and written in clear and plain language.

10.3 The TfGM web site will host a general privacy notice stating its principles and how it will apply them to protect the privacy of data subjects. This will be supported by a specific privacy notice for each data processing activity or processing by a functional area stating how these principles will apply in that case.

10.4 All privacy notices will include details of:

- Identity of the data controller and the data protection officer.
- Why the data is being collected? I.e. the purpose.
- Legal basis for collecting and the associated legislation where applicable.
- Description of what personal information is being collected.
- How is it collected.
- How will it be used.
- Who will it be shared with.
- What will be the effect of this on the individuals concerned.
- The source of the data where it is not from the data subject.
- Details of any transfers to third countries and safeguards.
- Details of the retention periods or criteria used to determine the retention period.
- Information about individuals' rights and how they can exercise those rights.
- Details of how to lodge a complaint with the Information Commissioner.
- Details of any automated decision making or profiling.

11. Data Protection by design and by default

11.1 Organisations are required to integrate data protection concerns into every aspect of their processing activities. This is 'data protection by design and by default'.

11.2 What this means is that at the design phase of any system, service, product, or process and throughout the lifecycle, privacy and data protection issues must be considered -this approach is data protection by design. Effectively Controllers must put in place appropriate technical and organisational measures designed to implement the data protection principles and integrate safeguards into the processing to meet TfGM requirements and protect individual rights.

The rights and freedoms of the particular data subjects whose personal data to be processed when designing new systems and processes must be considered.

11.3 In addition, controllers must ensure they only process data that is necessary to achieve the specific purpose. This is data protection by default and links to the principles of data minimisation and purpose limitation.

12. Data Protection Impact Assessments (DPIA)

12.1 A DPIA is an assessment tool that is used to identify and reduce the data protection risks of processing activities and are integral to data protection by design and by default approaches.

12.2 It is a legal requirement for a DPIA to be undertaken for processing that is large scale and/or likely to result in a high risk to individuals. This includes some specified types of processing. Further details on what constitutes high risk processing can be found here.

12.3 When assessing the level of risk, both the likelihood and the severity of any impact on individuals should be considered. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

12.4 A DPIA must be undertaken for any project within TfGM that requires the processing of personal data.

12.5 The Data Protection Officer should be consulted for guidance when any new or major changes to data processing activities are being considered.

12.6 Where a high risk has been identified that cannot be mitigate, the ICO must be consulted before commencing the processing

12.7 A DPIA should be started as early as is practicable in the design of the project, even if some of the process is still unknown. Updating the DPIA throughout the lifecycle of the project, will ensure that data protection and privacy are considered. It will also highlight areas that may have project completion implications as well.

12.8 It can also be necessary to repeat individual steps of the DPIA as the project process progresses because the selection of certain technical or organisational measures may affect the risks posed by privacy and data protection.

13. Employee Data

13.1 TfGM reserves the right to collect, store and process data about its employees that is relevant to their employment. This will include special categories of data.

13.2 This is necessary for monitoring TfGM's commitment to equality of opportunity, meeting employment law obligations, making trade union deductions, providing an occupational health and safety function and promoting the wellbeing of staff and ensuring payment of staff salaries and relevant deductions.

13.3 The Subject Access Request and Data Protection procedures provide further detailed guidance on how requests will be dealt with.

13.4 A register will be kept of all requests for information including Subject Access Requests.

14. Disclosure

14.1 Disclosure or sharing of information is subject to this policy. Disclosure of information will be in accordance with Legislation and in keeping with the TfGM Information Sharing Policy.

14.2 In most cases TfGM will only disclose information using the legal justification for processing and the Article 6 and 9/schedule 1 conditions of the GDPR. Where this is not possible, we will ask the data subject for consent to disclose.

14.3 Employees who inappropriately disclose or make any use of personal information either during or after their employment with TfGM will be in breach of both this policy and the legislation and as such may be liable to disciplinary action and prosecution.

14.4 TfGM encourages employees who are aware of or suspect malpractice to report these suspicions. The Whistleblowing Policy tells staff how to do this.

15. Data Breaches

15.1 Despite the wide range of security measures put in place by TfGM personal data breaches may still occur.

15.2 TfGM has a legal obligation to notify the ICO within 72hours of becoming aware of a data breach if it is likely to result in a risk to the rights and freedoms of data subjects. Failure to notify a breach of this nature could result in a financial penalty being imposed.

15.3. The DPO is responsible for assessing data breaches and determining if the ICO should be notified and where applicable notifying the data subject.

15.4 Personal data breaches including suspected breaches must be reported to the Information Governance Team and DPO immediately via the data breach process.

16 Children's data

16.1 A child is defined as anyone under the age of 18. Children's data merits special protection under data protection legislation. Children may not always be aware of the risks involved with the processing of their data, therefore it is important that when systems and

processes are designed that consideration is given to children's data processing and the specific protection that is required. The ICO has produced an Age Appropriate Design Code of Practice for online services which should be followed.

16.2 As with adult data a lawful basis is required to process children's data. Consent is one possible lawful basis however an alternative basis may be more appropriate and provide more protection for the child.

16.3 When offering online services to a child and consent is the legal basis then only a child aged 13 and over can give their own consent. For a child under this age then then consent must be obtained from the person with parental responsibility.

16.4 Privacy notices for children must be clear and written so that they are able to understand what will happen to their personal data, and what rights they have.

16.5 Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

16.6 If processing is likely to result in a high risk to the rights and freedoms of children then TfGM must do a DPIA.

17 Privacy and Electronic Communications

17.1 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches.

17.2 The DPA 2018/GDPR and Privacy and Electronic Communications both restrict the way organisations can carry out unsolicited direct marketing (that is, direct marketing that has not specifically been asked for).

17.3 The rules provide that if TfGM is planning a marketing campaign or planning to use cookies then the organisation must comply with the regulations. This includes ensuring that the use of someone's data is clearly outlined and such use is covered by the appropriate legal basis. TfGM must provide a simple way for the public to opt out of marketing messages if they wish to change their mind and have a system in place for dealing with complaints.

17.4 As a public body it is possible to use the public task legal basis for direct marketing if it can be demonstrated that the processing is necessary for a specific task (e.g. keeping the GM travelling public aware of facts during critical times such as Covid 19) or a function set down in law. Good practice recommendation from the ICO however is to get consent for all direct marketing regardless of whether PECR requires it or not.

17.5 The ICO has produced a draft Direct Marketing Code of Practice and TFGM will be expected to ensure that any Direct Marketing undertaken is compliant with this draft code and the subsequent final approved code.

17.6 To be compliant with DPA 2018/GDPR a lawful ground to collect and process cookies which identify an individual must be identified. People must be told the cookies are there and must be told what the cookies are doing and why. In addition, websites cannot use 'non-essential' cookies unless the consent of the user is expressly given - in other words, users must first opt-in before such cookies can be deployed.

17.7 Non-essential cookies are those which are used for analytical purposes or to assist with advertising. Essential cookies are generally those which enable an online checkout process to work properly - or if required for technical or security purposes.

17.8 If TfGM is processing data from direct marketing or use of cookies is of a type likely to result in high risk, then a DPIA must be undertaken before processing commences.

18. CCTV/Surveillance Systems

18.1 Surveillance cameras/systems can be privacy intrusive and may process an individuals' information i.e. their personal data. They are no longer a passive technology that only record and retain images, but are now a proactive one that can be used to identify people of interest and keep detailed records of people's activities, such as with ANPR cameras, traffic monitoring devices, body worn video, thermal cameras, unmanned aerial devices (drones) etc.

18.2 When using, or intending to use surveillance systems, TfGM must consider their obligations in relation to the Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act, the Human Rights Act 1998 (HRA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code). Any surveillance system must also comply with the ICO's CCTV code of practice.

18.3 Before introducing a new system or updating/upgrading an existing one a Data Protection Impact Assessment must be carried out which considers, privacy in a wider context than just the DPA, but considers the HRA and the impact on privacy rights. This will aid in

ensuring that the proposed use of a surveillance system has a lawful basis and is justified, necessary and proportionate.

19 Profiling and automated decision making

19.1 The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

19.2 Solely automated individual decision-making, including profiling with legal or similarly significant effects is restricted. However, there are a number of grounds that lift the restrictions and where one of these applies additional safeguards to protect individuals must be introduced

19.3 There is also specific information about automated decision making, including profiling that must be given to individuals and there are additional restrictions on using special category and children's personal data.

19.4 This type of processing is considered to be high-risk and therefore a Data Protection Impact Assessment (DPIA) must be carried out to identify and assess the risks before any processing commences.

20 Complaints about Personal Data

20.1 Any complaints received from a Data Subject regarding errors or inaccuracies in the data we hold about them, or that points out unfair uses of their data, must be reported to the IG Team immediately for processing.

20.2 An investigation of the complaint will be carried out to the extent that it is appropriate based on the merits of the specific case. The DPO will inform the data subject of the progress and the outcome of the complaint within a calendar month of receipt of the request.

21 Awareness and Training

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

21.2 TfGM will provide relevant training both on-line and face to face to ensure that staff understand the legislation and its application to their role. In addition to this the

protection and appropriate use of data will be subject of communications campaigns to employees and should be discussed at team meetings.

21.3 The compliance data for those members of staff completing/not completing the online eLearning courses is reported by the SIRO to ARAC at least twice a year.

22 Compliance and Monitoring

22.1 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.

22.2 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 data.protection@tfgm.com

22.3 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 assist in ensuring TfGM meets the requirements of the legislation.

22.4 The IG Team will undertake periodic checks to monitor compliance with the Policy within TfGM and its contracted Data Processors Results will be recorded and, where appropriate, action taken to enforce compliance and recommendations provided that strengthen compliance.

22.5 It is anticipated that Internal Audit will undertake periodic checks on TfGM's arrangements for complying with the Act.

22.6 An Information Risk Governance Group will meet at least quarterly and will receive reports from the DPO on all aspects of the implementation of this Policy.

22.7 A quarterly compliance report will be provided by the SIRO to the Audit and Risk Assurance Committee.

22.8 The quarterly and annual compliance report will be submitted to the Executive Board by the SIRO.

22.9 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.

17.10 The GMCA and TfGM will continue to review the effectiveness of this policy to ensure that it is achieving it intended purpose.

17.11 Any infringement of the Act will be treated seriously by TfGM and may be considered under disciplinary procedures.

Appendices

Appendix 1: Definitions

Automated Decision Making – is a decision made using automated means without any human intervention.

Data Controller – The person or organisation who (either alone or jointly with others) determines the purposes and means by which personal data are or are to be processed. In this instance the TfGM is the Data Controller.

Data Processing – means carrying out any operation or set of operations on the information or data whether or not by automate means such as:

- obtaining, recording, structuring, storage or holding the information or data,
- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available,
- alignment, combination, blocking, erasure or destruction of the information or data.

Data Processor – Any person or organisation, other than an employee of TfGM, who processes personal data on behalf of the data controller, e.g. someone contracted to TfGM to print documents containing personal data.

Data Subject – means the individual about whom personal (or sensitive personal data) is held. A data subject must be a living individual.

Information Asset – An information asset is a body of information which can be personal or non-personal data, defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively. Information assets have recognisable and manageable value, risk, content, and lifecycles. Information assets can be hard copy records, electronic records or records stored on any form of media, including databases, spreadsheets, documents, images, emails, websites etc.

Personal Data – means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier including name, identification number, location data or online identifier or to one or more factors specific to the physical, physiological, mental, genetic, economic, cultural, or social identity of that person.

Personal Data Breach - a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Profiling – profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation - 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

Special Category Data – This is personal data considered to be sensitive and is subject to much stricter conditions of processing. The special categories of data are:

- Race or Ethnic origin,
- Politics, political opinions,
- Religion/religious or philosophical beliefs,
- Trade union membership,
- Genetics,
- Biometrics (where used for ID purposes),
- Physical or Mental Health condition,
- Sex life,
- Sexual orientation.

Appendix 2: TfGM Related Policies and Procedures:

- Information Sharing Policy. – under review,
- Information Security Policy,
- Special Category Data Policy – in development,
- Information Rights Policy – in development,
- Confidential Waste Policy – under review,
- Freedom of Information Act Policy – in development,
- Records Retention Schedule,
- Data Quality Policy – in development,
- Disciplinary Policy,
- Employee Code of Conduct.

Appendix 3: Legal bases for processing

1. Legal bases for general processing of Personal Data

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the data controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This does not apply to processing carried out by public authorities, such as Universities, in the performance of their public tasks).

2. Legal bases for processing Special Category Personal Data

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and rights of the data controller or of the data subject in the field of employment and social security (subject to the Data Protection Act 2018);

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to safeguards;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016,

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 4 Further Information and Guidance

Data Protection Officer

Data Protection Officer –

Email: data.protection@tfgm.com

SIRO

Email: kath.wilson@tfgm.com

General enquires and Information Rights Requests

Information Governance Team

Email: data.protection@tfgm.com

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