GREATER**LONDON**AUTHORITY

GLA Data Protection Policy

Date of approval and issue	January 2020
Version	3.0
Approved by	Governance Steering Group

Changes from previous version	Significant revisions to reflect changes in legislation
Review date	January 2022
Senior owner	Executive Director Strategy & Communications
Document owner	Information Governance Manager and Data Protection Officer

Introduction

The General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 regulate the processing of any information that relates to an identifiable individual, including the obtaining, collection, retention, handling, use or disclosure of any such information, and covers data held in any format, including paper records and data held in a database or other electronic format.

Purpose

The objective of this policy is to ensure that:

a) All personal data processed by GLA complies with the requirements of data protection legislation and other relevant information governance legislation; and

b) GLA staff and employees are aware of their obligations when processing Personal Data on behalf of the Authority.

Definitions

- **Data Controller** – The organisation (alone, jointly or in common with other organisations) which determines the manner and purposes for which Personal Data is to be processed.

- **Data Processor** - Processes data on behalf of the Data Controller (other than an employee).

- **Data Protection Legislation** - General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 and, any other legislation in force from time to time in the United Kingdom relating to privacy and/or the processing of personal data. Data protection legislation governs the way in which Data Controllers can process an individual's Personal Data.

- **Data Protection Officer** - A statutory requirement of the GDPR is the appointment of a Data Protection Officer (DPO). The GLA DPO reports to GLA Governance Steering Group (which includes the GLA Chief Officer and GLA Senior Information Risk Officer). The GLA will ensure that the DPO is able to operate independently and is provided adequate resources to meet their obligations under GDPR.

- **Data Protection Principles** - A set of statutory requirements, which all Data Controllers are obliged to adhere to. The Principles balance the legitimate need for organisations to process Personal Data against the need to protect the privacy rights of the Data Subject.

- **Data Subject** - An individual who is the subject of Personal Data.

- **GLA staff** - Includes all GLA employees and elected Members, and any temporary, agency or contracted staff engaged by the Authority or working on behalf of the Authority, including staff working on behalf of Assembly Members and the GLRO in their capacities as separate data controllers to the GLA. It also covers any third parties with whom special arrangements (such as Data Processor, confidentiality or non-disclosure agreements) have been made.

- **Information Commissioner** - The regulator appointed by the Crown to promote public access to official information and protect personal information. Compliance with the Data Protection Legislation is enforced by the Information Commissioner.

- **Personal Data** - Any information relating to an identifiable person who can be directly or indirectly identified by that information, in particular by reference to an identifier, including name, identification number, location data or online identifier. Personal Data includes expressions of opinion and indications of intention, as well as factual information, and may include pseudonymised data where it is possible to attribute the pseudonym to a particular individual.

- **Personal Data Breach** - The loss, destruction, damage, theft, inappropriate use or unauthorised disclosure of Personal Data.

- **Processing/Processed** - Includes collecting, recording, storing, retrieving, transmitting, amending or altering, disclosing, deleting, archiving and destroying Personal Data.

Scope

The GLA, each individual London Assembly Member and the Greater London Returning Officer (GLRO) are, for the purposes of the GDPR, the Data Protection Act 2018, and for the purposes of this policy, separately registered data controllers.

This policy applies to all GLA Staff and to all Personal Data Processed by or on behalf of the GLA at any time, by any means and in any format.

Policy Statement

Under this policy, the GLA will:

a) Comply with Data Protection Legislation and adhere to the six Data Protection Principles, as described in the Annex to this policy

b) Comply with the statutory requirement to document its processing of Personal Data, including:
   i) The name and contact details of the Data Protection Officer
   ii) The purposes for which Personal Data are processed, and the legal basis for the processing
   iii) Descriptions of the categories of Data Subjects and Personal Data
   iv) The categories of recipients of Personal Data
   v) Details of transfers of Personal Data to third countries
   vi) Retention Schedules

vii) A description of the technical and organisational security measures protecting Personal Data

c) Comply with all other relevant legal requirements which apply to its processing of Personal Data, including:

i) The Human Rights Act 1998 and the requirement to act in a way which is compatible with the right to respect for private and family life in the European Convention of Human Rights and Fundamental Freedoms

ii) The Privacy and Electronic Communications (EC Directive) Regulations 2003

iii) The common law duty of confidence

d) Adhere to the requirements set out in the following standards, policies and guidance in order to support its compliance with Data Protection Legislation, including:

i) European Data Protection Board guidance on compliance with the requirements of the GDPR

ii) The Information Commissioner's guidance documents and Codes of Practice

iii) GLA Records Management Policy

iv) GLA Freedom of Information Guidance

v) GLA Information Security Policy

vi) The GLA Personal Data Incidents & Breaches Policy

vii) The GLA Code of Conduct

viii) The GLA Code of Ethics and Standards for Staff

e) Be open and transparent about how we Process Personal Data, providing clear privacy notices at the point data is collected, with access to additional supporting information through the GLA website

f) Implement appropriate structures, systems and processes to manage all Personal Data fairly and lawfully and in a way that ensures its integrity, accuracy, relevance and security

g) Not disclose Personal Data to third parties except where disclosures are permitted by, or required by, law

h) Consider and respond to requests from individuals who object to, or seek to restrict the Processing of their Personal Data, and consider and respond to requests to rectify or erase Personal Data

i) Ensure our procurement processes and contractual arrangements with external service providers include adequate measures to ensure compliance with the Data Protection Principles and associated requirements outlined in this policy, and monitor compliance with those measures

j) Follow the principles of Privacy by Design and Default to help ensure that Privacy and Data Protection is a key consideration in the early stages of any project, and then throughout its lifecycle. Conduct Data Protection Impact Assessments when considering the adoption of new technologies or any potential high-risk processing of Personal Data

k) Approach the identification and management of Privacy Risk in the same way as financial and operational risk

l) Give members of the public the opportunity to consent to receiving future marketing communications at the point at which their Personal Data is first collected; and within any

marketing communications, provide a simple and transparent process through which they can unsubscribe

m) Ensure that requests from customers to change the use of their data for the purposes of marketing and/or the provision of service updates will be acted on promptly

n) Ensure that any complaint about the GLA's processing of Personal Data or non-compliance with this policy is passed to the GLA Information Governance Team DPO. The complaint will be dealt with promptly and in line with process outlined within the GLA's Data Subject Rights Procedure

o) Require GLA staff directly involved in the Processing of Personal Data to complete appropriate training on a regular basis

p) View serious or repeated breaches of this Policy by a GLA member o staff as misconduct which will be managed and resolved in accordance with relevant disciplinary policies and procedures

q) Ensure use of CCTV and similar equipment is in accordance with the requirements of the Information Commissioner's Surveillance Camera Code of Practice and the Home Office Surveillance Camera Code of Practice

Responsibilities for privacy and data protection compliance

All GLA staff are responsible for actively supporting compliance with this policy and should only process Personal Data for legitimate business purposes directly related to the performance of their duties.

- GLA Senior Managers are responsible for:

    - Ensuring that GLA Staff within their teams and area of responsibility are aware of this policy and are adequately trained in the handling of Personal Data
    - The assessment and reporting of privacy risks linked to the Processing of Personal Data within their area of responsibility and ensuring that Data Protection Impact Assessments are carried out where necessary
    - Implementing and documenting appropriate procedures to ensure Processing of Personal Data within their teams and area of responsibility is compliant
    - Advising the GLA DPO of changes in the Processing of Personal Data, in order to maintain the Data Protection documentation referred to above.

- The Data Protection Officer is responsible for:

    - Providing advice and guidance on the implementation and interpretation of this Policy and/or Data Protection Legislation, including the assessment of Data Protection Impact Assessments and the provision of suitable Data Protection training
    - Promoting, monitoring, auditing and enforcing compliance with this Policy, Data Protection Legislation and any other related statutory, common law or regulatory requirements which apply to the GLA

- Providing a first point of contact for members of the public and individuals whose data is processed, and investigating and resolving complaints about the GLA's non-compliance with Data Protection Legislation and/or this Policy
- Liaising with the Information Commissioner's Office (ICO) on any matter relating to the GLA's compliance with Data Protection Legislation and/or this Policy
- Maintaining the documentation concerning the GLA processing of Personal Data
- Maintaining procedures for recording, reporting and responding to a Personal Data Breach

- All GLA Staff are responsible for reporting actual or suspected Personal Data Breaches to GLA Information Governance Team and DPO in accordance with the GLA Personal Data Incidents and Breaches Policy.

- The GLA Technology Group and Information Governance Team are jointly responsible for advising the business on the technical measures and controls required to protect the security and integrity of Personal Data Processed by the GLA using electronic information and communications systems.

- Internal Audit is responsible for auditing the business processes, operating procedures and working practices of the GLA for the purposes of monitoring compliance with this policy.

- It is **not** the responsibility of the GLA DPO to apply the provisions of the Data Protection Legislation; this is the responsibility of all GLA Staff, Senior Managers and users of Personal Data. GLA Staff are required to be aware of their responsibilities under the Data Protection Legislation and its impact on the work they undertake on behalf of the Authority.

- All staff are responsible for ensuring that:

  - Any personal data they hold, whether in electronic or paper format, is kept securely.
  - Personal data is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Data Protection Officer

The GLA, each individual London Assembly Member and the Greater London Returning Officer (GLRO) are, for the purposes of the GDPR, the Data Protection Act 2018, and for the purposes of this policy, separately registered data controllers.

The GLA Data Protection Officer for the GLA, London Assembly Members and the GLRO is Ian Lister, the GLA Information Governance Manager.

Procedures, guidance and processes

This policy will be supported by specific policies, process and guidance made available to GLA Staff and published on the GLA Intranet.

Approvals and amendments

This policy was approved by the GLA Governance Steering Group on 14 January 2020

This policy will be subject to periodic review as considered appropriate by GLA DPO and Governance Steering Group.

Annex A - Principles relating to processing of personal data

Under Article 5 of GDPR, personal data should be:

a) processed fairly and lawfully and in a transparent manner in relation to the data subject

The GLA will only process personal data where we have identified a lawful basis for that processing, and in any situation where individuals provide the GLA with their Personal Data for the first time, or if it is processed for a new purpose, they will be informed of:

- the identity and contact details of the Data Controller and Data Protection Officer;
- the purposes and lawful basis for the processing;
- any the recipients or categories of recipients of the personal data;
- the period for which the personal data will be stored;
- the rights of the individual regarding the processing of their personal data including the rights to access and data portability, rectification and erasure, restriction of processing and the right to object to processing.
- the consequences of not providing the personal data required under statute or for contractual purposes; and
- the existence of, and rights relating to, automated decision-making including profiling.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

The GLA will only process Personal Data for the purpose(s) for which that Personal Data was provided and for which the Data Subject was previously informed of, and it will not be used for any other purpose that is incompatible with the original purpose(s). Subject to appropriate safeguards being agreed with the Information Governance Team, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

The GLA will always aim to ensure that only the minimum Personal Data necessary for the purpose is processed and will not seek collect or retain any Personal Data on the basis that it might be useful in the future. There should always be a legitimate business reason for the Processing of Personal Data linked to a specific purpose.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

The GLA will consider Personal Data to be inaccurate where it is incorrect or has the potential to be misleading. We will take reasonable steps to ensure the accuracy of any Personal Data and to accurately amend, update or correct that Data.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Teams across the GLA must implement appropriate retention periods and ensure that Personal Data is securely destroyed once the purpose(s) for processing the Personal Data has come to an end; and there is no legal requirement or valid business or operational reason for its continued retention.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures agreed with the Information Governance Team.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Standard contractual clauses on data protection must be used in any circumstances where any Processing of Personal Data is to be carried out by a service provider or other third party on behalf of the GLA.

The Information Governance Team and GLA DPO must be consulted in the early stages of any project or proposed change to a business process that has any significant implications for the Processing of Personal Data.

GLA Staff must report any actual or suspected incident, which either has or is likely to, result in the loss, theft, unauthorised disclosure, accidental destruction or other compromise of Personal Data directly to the GLA DPO in accordance with the GLA Personal Data Incidents and Breaches Policy.

The GLA will continue to comply with the restrictions in the Data Protection Act 1998 on the transfer of Personal Data outside the European Economic Area (the 28 member states of the European Union plus Norway, Iceland and Lichtenstein). The Information Governance Team and GLA DPO **must** be consulted in advance of any such transfers being undertaken or agreed.