GREATER**LONDON**AUTHORITY

CCTV, Body Worn Camera and Access Control System Policy

Document Reference No.	GLAFM069A
This Issue Number	2
First published	May 2022
Date of this Revision	October 2026
Next Revision due	October 2027
Compiled by	Deputy Security & Operations Manager
Reviewed by	Data Protection Officer
Approved by	Security & Operations Manager

Contents

1.0 Introduction

2.0 General Data Protection Regulations (GDPR)

- 2.1 The seven key Data Protection Principles
- 2.2 GDPR lawful basis and special category data
- 2.3 GDPR Article 30

3.0 CCTV and Access Control Systems Privacy Statement

4.0 CCTV

- 4.1 Purpose of CCTV usage
- 4.2 Retention period – CCTV
- 4.3 Surveillance Camera Code of Practice
- 4.4 Body Worn Cameras
- 4.5 Audio Recording

5.0 Electronic Access Control

- 5.1 Category of personal data
- 5.2 Retention Period Electronic Access Control

6.0 Right of the Data Subject

7.0 GDPR Data Breaches

8.0 Policy Review

1.0 Introduction

This policy details the purpose, use and management of the CCTV including Body Worn Cameras & electronic Access Control Systems in order to ensure that the Greater London Authority (GLA) continues to comply with the relevant UK legislation and the current Information Commissioner's Office Surveillance Camera Code of Practice. The GLA will have due regard to the applicable legislation detailed within this document.

The GLA has in place Closed Circuit Television surveillance (CCTV), including Body Worn Cameras (BWC) with audio and electronic Access Control Systems installed within and around its premises at the City Hall, in Kamal Chunchie Way, London E16 1ZE and in use at Trafalgar Square London and Parliament Square Gardens (body worn cameras only).

The use of CCTV, Body Worn Cameras and electronic Access Control Systems is an essential part of the layered protective security measures deployed across the GLA's core sites at City Hall and Trafalgar Square. At Parliament Square Gardens there are no fixed CCTV cameras, instead Body Worn Cameras are used when necessary.

The data captured on CCTV and electronic Access Control System are classed as identifiable personal data. GLA is committed to protecting an individual's privacy and personal data when using GLA facilities. Under the data protection legislation, the GLA is only allowed to use personal information if there is a valid reason (known as the lawful basis) to do so. The lawful basis for collecting personal data is set out in the paragraphs below.

The use of all personal data by GLA is governed by:

- Surveillance Camera Code of Practice
- The UK General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations (PECR)
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act (2000)
- Protection of Freedoms Act (2012)

Every member of staff has a responsibility to adhere to the data protection principles as defined in the GDPR, and to this policy. Any questions about this policy or an area of concern about data protection matters, should be addressed to the GLA's Data Protection Officer (DPO).

The DPO email address is: data.protection@london.gov.uk.

This CCTV and Access Control System Policy should be read in line with the GLA's data protection policy.

Security and Operations Management, is responsible for the overall management and operation of the CCTV & electronic Access Control Systems, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.0 General Data Protection Regulations

2.1 The seven key Data Protection Principles

There are seven Data Protection Principles defined in Article 5 of the GDPR 2018. These require that all personal data shall be:

a) Processed in a lawful, fair and transparent manner.
b) Collected only for specific, explicit and limited purposes ('purpose limitation').
c) Adequate, relevant and not excessive ('data minimisation').
d) Accurate and kept up to date where necessary.
e) Kept for no longer than necessary ('storage').
f) Handled with appropriate security and confidentiality.
g) The controller shall be responsible for and be able to demonstrate accountability with the principles.

The GLA is committed to upholding the Data Protection Principles, this applies to all personal data controlled by the GLA which must be processed in accordance with these principles.

2.2 GDPR lawful basis and special category data

All processing of personal data must include the lawfulness of processing defined in Article 6 of the GDPR 2018.

Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR 2018) must further be processed only in line with one of the conditions specified in Article 9(2).

Where processing is based on consent, the data subject has the option to easily withdraw their consent.

The data captured on CCTV and electronic Access Control System are classed as identifiable personal data. GLA is committed to protecting an individual's privacy and personal data when using GLA facilities.

The 'legal bases' relied on to process the personal data we collect via CCTV or BWCs are as follow:

- Article 6(1)(c) (legal obligation)
- Article 6(1)(e) (public task)
- Article 6(1) (d) (vital interests), in emergency situations only.

For special category data, we rely mainly on the condition at Article 9(2)(g) - Reasons of substantial public interest within the Data Protection Act 2018. However, there may be occasions where we will rely on other conditions such as:

- Article 9(2)(b) (employment, social security and social protection) with the Data Protection Act 2018 Schedule 1 Part 1 condition
- Article 9(2) (c) (vital interest) in an emergency

- Article 9(2) (f) for legal claims or judicial acts

Data collection processes will be regularly reviewed by the GLA to ensure that personal data collected and processed is kept to a minimum.

The GLA will keep the personal data that is collected, used and shared to the minimum amount required to be adequate for its purpose.

Where the GLA does not have a legal obligation to retain some personal data, it will consider whether there is a need for it to hold it.

The GLA will retain personal data only for as long as it is necessary to meet its purpose. The approach to retaining and erasing data no longer required will be specified in the retention policy and schedule. This schedule will be reviewed annually.

In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.

Anonymisation and pseudonymisation of personal data stored or transferred should be considered where it is possible to do so. It must be noted however that information that has been truly anonymised is not caught under the provisions of the data protection law.

Paragraph 4.2 sets out the retention periods for CCTV data and paragraph 5.2 for electronic access control system data.

2.3 GDPR Article 30

The GLA will maintain a Data Processing Register as required by Article 30 of the GDPR 2018 to document regular processing activities.

The Data Protection Officer (DPO) has the specific responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation.

The DPO will ensure that the Information Asset Register and the Record of Processing Activities (RoPA) are kept up to date and demonstrates how the data protection principles are adhered to by our activities. Individual members of staff have a duty to contribute to ensure that the measures outlined in the Register are accurately reflected in our practice.

All employees, volunteers, consultants, partners or other parties who will be handling personal data on behalf of the GLA will be appropriately trained and supervised where necessary.

The collection, storage, use and sharing of personal data will be regularly reviewed by the DPO.

The GLA will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.

Where there is likely to be a high risk to individuals' rights and freedoms due to a CCTV related processing activity, the GLA will first undertake a Data Privacy Impact Assessment (DPIA) and if necessary, the Data Protection Officer will consult with the ICO prior to processing.

All staff, contractors, temporary workers, consultants, partners or anyone else working on behalf of the GLA and handling personal data are bound by the data protection legislation and this policy.

Where any contractor, temporary worker, consultant, or anyone else working on behalf of GLA fails in their obligations under this Policy, they shall indemnify GLA against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

The GLA is legally required to have a DPO as the number of staff exceeds 250 staff and as such the GLA is classed as a Tier 3 Data Controller. The Data Protection Officer role is assigned to a permanent member of staff on a full-time basis.

The DPO supports the GLA in:

a) Monitoring internal compliance.
b) Informing and advising on data protection obligations.
c) Providing advice regarding Data Protection Impact Assessments
d) Acting as the main contact point for data subjects and the Information Commissioner's Office.

The DPO advises the Executive Director of Corporate Resources and Business Improvement and reports to Senior Management on data protection matters. The DPO is easily accessible as a point of contact for staff for data protection issues and is identified as the first point of contact in the privacy notice and other external material.

While this CCTV and Access Control System Policy help to demonstrate how the GLA seeks to comply with data protection legislation related to this subject, it is the responsibility of members of staff operating and using the equipment and systems to comply with this policy.

In addition, staff should be aware of and adhere to other policies around the acceptable usage of IT systems, guidance issued in relation to cyber security and the use of personal data. These details can be found on the GLA intranet by searching IT Policies and Procedures.

3.0 CCTV and Access Control Systems Privacy Statement

This Policy applies to personal data collected by CCTV, Body Worn Cameras and electronic Access Control Systems at City Hall, London, E16 1ZE and Trafalgar Square and Parliament Square Gardens. The information in this policy forms part of the GLA privacy notice. The privacy policy is available on the GLA's website.

The systems are owned by the GLA and managed by its security team based at City Hall, London and its appointed agents at Trafalgar Square and Parliament Square Gardens and at other external temporary event venues.

In line with data protection, the GLA is the data controller for the CCTV and electronic Access Control Systems at City Hall. The GLA is the data controller for CCTV at Trafalgar Square. The GLA is data controller for the use of body worn cameras at City Hall, Trafalgar Square and Parliament Square (used by its security staff). The GLA is registered with the Information Commissioner's Office and the registration number is Z4760661. The GLA has no CCTV or access control at Parliament square.

Where these systems can process data which by itself or together with other data available to the GLA can be used to identify an individual, this is known as personal data.

This document sets out how the GLA uses personal data. Data subjects can contact the GLA at data.protection@london.gov.uk with any questions, including specific questions about whether or not a particular site has a CCTV and/or electronic Access Control System installed and whether data processors are operating that site on our behalf.

The GLA takes the security of personal data very seriously and takes a stringent approach to data protection which includes taking appropriate technical, physical and organisational measures to protect and store it. The GLA regularly evaluates whether it is necessary and proportionate to use CCTV systems at each of the sites for which it has responsibility as a Data Controller. Each site that uses CCTV has had a privacy impact assessment conducted and audits are undertaken to ensure that correct legal procedures are followed. Regular legitimate interest assessments are also conducted.

Prior to disclosing any CCTV footage, officers seek the advice of the Data Protection Officer to protect personal data from inappropriate or wrongful disclosure.

Data will not be processed or stored outside of the European Economic Area (EEA).

4.0 CCTV

4.1 Purpose of CCTV usage

The lawful basis for processing personal data using CCTV is provided above at paragraph 2.2. The GLA will use the data obtained from CCTV images for the purposes set out below:

a) Good property management
b) Maintaining the security of the premises
c) The prevention and detection of crime and the prosecution of offenders
d) To monitor goods and services.
e) For health and safety
f) For Protecting the rights, property and for the personal safety of the occupiers of the premises, including staff, tenants, visitors and members of the public.
g) When an individual exercises their rights under data protection law and makes a request.
h) When an individual makes a complaint under the Data Use & Access Act 2025 about the handling of their personal data

i) Based on an individual's consent if the person asks the GLA to disclose their personal data to other people or organisations such as a company handling a claim on their behalf, or otherwise agree to disclosures
j) For the security of equipment and vehicles

4.2 Retention Period – CCTV

CCTV recorded images and where applicable, audio recordings, will be kept for a limited period only, usually a maximum of 30 days and are then automatically erased. The exception being where recordings are required for evidential purposes or another legally valid reason including responses to data subject access requests.

4.3 Surveillance Camera Code of Practice

The operation of the CCTV system by the GLA is also guided by the Surveillance Camera Code of Practice, Surveillance Camera Code of Practice, issued by the Secretary of State under Sections 29 to 31 of Protection of Freedoms Act 2012.

The CCTV systems used by the GLA, and its agents are operated by SIA trained and licensed security staff who hold Public Space Surveillance licenses.

4.4 Body Worn Cameras

Body Worn Cameras with integral audio recording (BWC) are used by the GLA to:

- Improve security staff and Heritage Warden safety
- Enhance public safety
- Moderate people's behaviour in potentially volatile situations and enforcement activities
- Provide evidence for prosecution / defence
- Deter anti-social behaviour and breaches of byelaws and the Police Reform and Social Responsibility Act
- Provide evidence for post-incident analysis and investigations

BWCs may be used by the Heritage Wardens at Trafalgar Square and Parliament Square and GLA security staff and contractors at City Hall and external events. BWC's are only switched on when deemed appropriate by the officer wearing the BWC or their managers to be contributing to the above aims.

When BWCs are switched on there is a visual indicator to show that recording is taking place. The operator will also take reasonable steps to inform any person in front of them that recording is taking place, although where there are large crowds or in a very dynamic situation this may not always be possible.

4.5 Audio Recording

It is recognised that audio recording can be viewed as more intrusive and a greater invasion of privacy the CCTV alone, therefore audio recording is only deployed in places where the benefits outweigh the intrusion.

Audio recording via CCTV cameras is enabled in specific areas where there is a higher likelihood of an incident taking place that could result in physical harm to staff or visitors or when accurate and reliable evidence is required for prosecutions or for an inquiry. Those working in these areas are professional security staff who are briefed on the reasons for the recording so that they understand the protections it will provide to them and others. To make members of the public aware that audio recording is in place, in the areas they will pass through or visit, appropriate signage is displayed.

The areas covered by audio enabled CCTV cameras are:

- City Hall Search and Screening Facility – this is a dedicated room where security search and screening take place of all visitors coming into City Hall. This facility is an area where threats may be made, acts of violence occur or attempts at deception may take place and it is important that accurate evidence of incidents is captured.
- Security Control Room – this is the nerve centre of security operations at City Hall and is where the response to a critical incident is initiated, co-ordinated and managed. In a critical incident life safety decisions are taken by control room staff, and it is important for the post incident inquiry to understand when and why decisions were taken. Audio visual recordings will help provide clarity and context to the decision that are made and actions that are taken. This will provide a far more accurate account compared individual's memories of events, where recollections may differ, particularly where staff are operating in a pressurised environment.

Audio recordings made through the CCTV system are not available for review by the control room staff in the same way that they can review live CCTV images. Recorded footage is classified as confidential and access is limited to authorised security personnel. The release, sharing, or disclosure of recordings to any other party will only be permitted where there are a legitimate operational or investigative requirement and where appropriate authorisation has been obtained.

5.0 Electronic Access Control

5.1 Category of personal data

The category of identifiable personal data (directly or indirectly) that will be collected directly from CCTV footage may include a combination of the following dependent on the system itself and its objectives:

- name
- Photographic image
- Employer
- Position within that organisation
- Work location
- Contact details

The electronic Access Control System may record the days / times that staff/visitors enter and leave through access-controlled doors. This information will not be used to make any automated decisions concerning GLA employees.

Prior to any of GLA employee data being entered or processed by or into an access control system they will be advised of the exact content of the required data and the purposes for which their data will be used. Staff will have the right to question why the data is required and to object to anything that they do not want to be processed. By accepting a GLA security pass to facilitate access to designated premises, GLA employees agree that their personal data will be used in the manner described above.

Where GLA employees provide consent to their personal data being processed, they will have the right to withdraw that consent at any time, by returning the GLA security pass in their possession.

5.2 Retention Period – Electronic Access Control

In addition to the use of personal data for the purposes of access control, data will only be kept within the access control system for the duration of time during which an individual is employed by the GLA and needs to use the system to gain access to premises. After this time, the data will be deleted from the system.

For example, when a person is about to leave the organisation, they will return their security pass which operates the access control system, and their card will be cancelled on the system, the card destroyed, and their data deleted. In the event that the security pass is not returned, the card will still be cancelled and data deleted when notification of the leaver is received.

6.0 Rights of the data subject

Under data protection law, data subjects have certain rights:

- Right to be informed. The right to be told how their personal data is used in clear and transparent language.
- Right of access. The right to know and have access to the personal data we hold about them.
- Right to data portability. The right to receive their data in a common and machine-readable electronic format.
- Right to be forgotten. The right to have their personal data erased.
- Right to rectification. The right to have their personal data corrected where it is inaccurate or incomplete.
- Right to object. The right to complain and to object to processing.
- Right to purpose limitation. The right to limit the extent of the processing of their personal data.
- Rights related to automated decision-making and profiling. The right not to be subject to decisions without human involvement.
- Right to withdraw their consent

- Right to make a complaint to the Authority and subsequently to the Information Commissioner's Office.

The GLA will uphold individuals' rights under data protection law and allow them to exercise their rights over the personal data that the GLA holds about them. The GLA's CCTV privacy notice re-directs users to the GLA's 'Your privacy rights' page, which will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.

Any request in respect of these rights should preferably be made in writing to data.protection@london.gov.uk but verbal requests will also be accepted. Verbal requests will be confirmed in writing or another requested format to ensure it is clearly understood.

There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive', in which case administrative costs can be recovered.

Requests that are 'manifestly unfounded or excessive' can be refused. The GLA will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.

The GLA will respond to the request within one month from the date of request, unless the request is complex. The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.

The DPO has procedures for responding to requests where necessary, for example, for facilitating Data Subject Rights Requests.

7.0 GDPR Data Breaches

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. The likelihood of a breach occurring is low because of the systems control and procedures in place, such as restricted access to both the CCTV and Access Control Systems

All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:

- Loss or theft of devices or data, including information stored on USB drives or on paper.
- Hacking or other forms of unauthorised access to a device, email account, or the network.
- Disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients, email addresses.
- Alteration or destruction of personal data without permission.

Where a member of staff discovers or suspects a personal data breach in relation to CCTV or electronic access control, this should be reported to the DPO as soon as possible.

The Security and Operations Manager will then take the lead in investigating the breach supported by the DPO and present the findings and recommendations for preventing a re-occurrence to the Head of Facilities Management and Executive Director of Corporate Resources and Business Improvement.

Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

Where there is also a likely high risk to individuals' rights and freedoms, the GLA will inform those individuals without undue delay.

The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

8.0 Policy Review

The GLA's usage of CCTV and electronic Access Control systems and the content of this policy shall be reviewed annually by the Security and Operations Manager and Data Protection Officer with reference to the relevant legislation or guidance in effect at the time.