Policy & Standards for CCTV Operation

Version 7.1

Approved by the Board of Governors

Last Amendment: February 2026

The London School of Science and Technology ("LSST", "the School") seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors and contractors, whilst within or situated on the premises. To this end, CCTV cameras and recording devices are deployed within School to assist in the prevention, investigation and detection of crime, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), public, employee and student safety and monitoring the security of LSST premises.

This Policy document has been implemented to ensure that the deployment and control of CCTV resources is proportionate and lawful under the terms of the UK GDPR and the Data Protection Act 2018, the Data (Use and Access) Act 2025, and the CCTV Codes of Practice.

This Policy should be read in conjunction with the LSST Employee Data Protection and Records Management Policy and Data Protection Policy (Students).

Document Information

Document owner(s)*:	Head of Operations
Date of next review:	September 2026
Document Status:	Approved
Dissemination:	For general publication

*The document owner is responsible for maintaining and updating the content of this document and ensuring that it reflects current practice at the School.

Contents

1. Introduction

1.1. This document details the operating policy and standards for the closed-circuit television (CCTV) systems installed at LSST in accordance with the requirements of the GDPR and the Data Protection Act 2018 and the Code of Practice (CCTV Code) issued by the Information Commissioner.

1.2. The operational requirements for the CCTV systems and each camera in use across the School are to be documented in a "CCTV Operational Report", kept and maintained by the Head of Operations.

1.3. System Description

1.3.1. The CCTV systems installed in the School comprises of fixed cameras. These cameras provide fields of view encompassing approaches to the School's entrance and internal communal and secure areas. The majority of the CCTV cameras are networked for remote operation from a centralised Security Control room where digital hard disk recorders provide data management and recording facilities. Where software remote view facilities are provided to named system users elsewhere at the School, access to the systems is password protected.

1.4. Purpose of the System

1.4.1. The purpose of the CCTV system in use at LSST is to enable the prevention, investigation and detection of crime and monitoring of the security and safety of LSST premises.

1.5. Operating Principles

1.5.1. To ensure compliance with DPA, personal data, including images recorded on the CCTV system, must at all times be processed in line with the following Data Protection Principles:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with the purpose of the systems
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure
- Not transferred to countries outside of the EEA without adequate protection

1.6. To Whom this Document Applies

1.6.1. LSST (the "Data Controller") and its employees who operate, or supervise the operation of the CCTV system at LSST, namely Security Officers and any authorised persons.

2. Policy

2.1. Scope

2.1.1. This Policy applies to all parts of the School.

2.1.2. This system is used for the purposes of monitoring room usage and to assist with the use of audio-visual equipment. The owners of this system are responsible for ensuring appropriate signage is displayed in the areas of use explaining the purpose of the cameras & CCTV System.

2.1.3. Personal Data (i.e., Images of individuals obtained by the LSST CCTV system) may only be used in connection with the purpose set out in section 1.2.

2.1.4. The ability to view live and historical CCTV data available via network software is only to be provided at designated locations and to authorised persons. The Head of Operations is responsible for the evaluation of such locations and authorised persons against the requirements of this Policy document and is to maintain a record of all locations and authorised persons.

2.1.5. Except where a request has been granted for third party access to certain specified recorded CCTV images (see below), CCTV images are not to be displayed in the presence of any unauthorised person or where such images may be inadvertently viewed by any unauthorised person. Where images are accessed or monitored on workstation desktops, the CCTV screen is to be minimised when not in use or unauthorised persons are present. Workstation screens must always be left locked out when unattended.

2.1.6. For the purposes of viewing CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of LSST who has an operational responsibility for the prevention, investigation and detection of crime and/ or the monitoring of the security and safety of the premises at LSST.

2.1.7. No images may be captured from areas in which individuals would have an expectation of privacy (i.e., toilets, changing facilities etc.).

2.1.8. At all times the operation of the CCTV system is to be conducted in accordance with the procedures set out in this document.

2.1.9. The Head of Operations is responsible for ensuring that the CCTV system and camera specifications for new installations at LSST comply with the DPA and the CCTV Code.

2.1.10. Only the appointed contractor for the School's CCTV system may be used in installing or maintaining the CCTV system.

2.1.11. Changes in the use of the CCTV system may only be implemented in accordance with the DPA and the CCTV Code. The Head of Operations must be consulted before any changes take place.

3. Operating Standards

3.1. Processing CCTV Images

3.1.1. It is imperative that access to and the security of CCTV images are managed in accordance with the requirements of the DPA and the CCTV Code. At all times the standards set out below are to be applied.

3.1.2. CCTV images shall not be retained for longer than necessary. Data storage is automatically managed by the CCTV digital records which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces an approximate 28-day rotation in data retention.

3.1.3. Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal proceedings), the images will be erased following the expiration of the retention period.

3.1.4. If CCTV images are retained beyond the retention period, they will be stored in a secure place to which access is controlled and will be erased when no longer required.

3.2. Quality of Recorded Images

3.2.1. Images produced by the recording equipment must be as clear as possible in order to ensure that they are effective for the purpose for which they are collected. The standards to be met under the CCTV Code are set out below.

- Recording features such as the location of the camera and/or date and time reference must be accurate and maintained.
- Cameras must only be situated so that they capture images relevant to the purpose for which the system has been established.
- Consideration must be given to the physical conditions in which the cameras are located i.e., additional lighting or infrared equipment may need to be installed in poorly lit areas.
- Cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept.
- As far as possible, cameras must be protected from vandalism in order to ensure that they remain in good working order. Methods used may vary from

positioning at height to enclosure of the camera unit within a vandal resistant casing.

3.3. Appropriate Signage

3.3.1. Signs must be placed so that members of the public are aware that they are entering a zone which is covered by CCTV cameras. Such signs must:

- Be clearly visible and legible
- Be of a size appropriate to the circumstances

4. Access to/Disclosure of CCTV Images

4.1. Requests from third parties (i.e., unauthorised persons) for access to or disclosure of (i.e., provision of a copy) of images recorded on the CCTV system will only be granted if the requestor falls within the following types of person/organisation:

- Data Subjects (i.e., persons whose images have been recorded by the CCTV system).
- Law enforcement agencies (where the images recorded would assist in a specific criminal case).
- Prosecution agencies (including School Directors undertaking Staff or Student disciplinary proceedings).
- Relevant legal representatives of data subjects.

4.2. The contact point indicated on the CCTV signs around LSST should be available to members of the public during normal business hours. Employees staffing the contact point are to be familiar with this document and the procedures to be followed in the event that an access request is received from a Data Subject or a Third Party.

4.3. Request from a Data Subject for Access/Disclosure

4.3.1. Data Subjects (i.e., persons whose images have been recorded by the CCTV system) have various rights under the DPA, including the right to be informed that personal data (i.e., images of themselves) are being recorded and the right to view such images. Should any person visiting LSST have any questions concerning the operation of the CCTV system or their rights with respect to any images of them recorded by the systems, the procedure set out below must be complied with.

4.3.2. The Data Subject should be directed to LSST's Registry and/or Data Protection Officer (for students) and LSST's HR department (for staff).

4.3.3. The Data Subject should be provided with a copy of the Information Leaflet attached at Annex A, which describes the purpose and operation of the CCTV system at LSST.

4.3.4. Should the Data Subject wish to access CCTV images of themselves they should be provided with a copy of the Subject Access Request (SAR) Form, which is attached at Annex B. This will enable them to make a formal request to view / receive copies of images of themselves.

4.3.5. Data subjects are entitled to request a copy of the personal data held about them by LSST. Any data subject wishing to exercise this right should complete the Subject Access Request (SAR) Form, which is available via the Student Portal where applicable, and submit the completed form to the Registry at registry@lsst.ac (for students) or hr@lsst.ac (for staff).

4.3.6. On receipt of a Subject Access Request, the Registry or HR department will log the request and coordinate its processing in line with LSST's data protection procedures. The request will be shared with the School's appointed Data Protection Officer as soon as possible to ensure appropriate oversight and compliance.

4.3.7. LSST will respond to Subject Access Requests as quickly as possible and, in any event, within one month of receipt. Where a request is complex or where multiple requests are received from the same data subject, LSST may extend the response period by up to a further two months. In such cases, the data subject will be informed within one month of receipt of the request and advised of the reasons for the extension.

4.3.8. The Registry or HR department, will liaise with the Head of Operations in order to:

- Determine whether the request should be complied with.
- Ensure that the relevant images are located.
- Determine whether third party images (i.e., images of persons other than the Data Subject) are contained within the images.
- Ensure that any third-party images are disguised or blurred before access or disclosure is granted.

4.3.9. The Registry or HR department must ensure that a written acknowledgement is sent to the Data Subject as soon as practicable and in any event within 21 days of receipt of the completed SAR Form. The written acknowledgment will contain the following:

- The name of the Data Subject.

- A request for further information to enable identification of the Data Subject or relevant images (if necessary).

- A confirmation of the start date for the response period (see below).

4.3.10. SARs are to be processed as soon as practicable and in any event within 30 days of receipt of sufficient information to enable identification of the Data Subject and/ or relevant images.

4.3.11. Once the images have been located and the Registry or HR department, have determined that a SAR can be complied with, the data requestor must be provided with written notice containing the following:

- The name of the Data Subject.

- A description of personal data (i.e., images of the Data Subject recorded on the CCTV system at LSST and the period during which they were recorded.

- If the data requestor elected in their completed SAR Form to view the images at LSST, an invitation to contact the Registry or HR department, to arrange a viewing of the images during normal business hours.

- If the data requestor elected in their completed SAR to receive a copy of the requested images, references to a digital device being enclosed which contains the requested images and the blurring of any third-party images (if applicable).

4.3.12. If the Data Subject elected in their completed SAR form to view the images at LSST an entry needs to be made in the CCTV Operating Log Book recording:

- The name(s) of the data requestor and any other attendees.

- The date and time of the viewing.

- The location where the viewing took place.

4.3.13. If the Registry or HR department, determine that a SAR cannot be complied with, data requestor must be provided with written notice containing the following recording:

- The name of the Data Subject.

- The reason for refusing to grant access to / supply the images requested (e.g., compliance with the request would, or would be likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders; the images have already been erased etc.).

4.4. Request from a Data Subject to Prevent Processing/Automated Decision Taking

4.4.1. In addition to rights of access, Data Subjects also have rights under the DPA to prevent processing (i.e., monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person, or prevent automated decision taking (i.e., through the use of visual recognition software) in relation to that person. It is unlikely that either ground would apply to the operation of the CCTV system at LSST, however, should any person visiting LSST have any concerns regarding the operation of the CCTV system, the following procedure must be complied with.

4.4.2. The Data Subject should be directed to the Registry or HR department who will determine whether the Data Subject is making a request to prevent processing or automated decision making. If the Registry or HR department and the Data Protection Officer determine that the Data Subject is instead making a SAR, the procedure set out in paragraph 4.1 above will be followed.

4.4.3. The Registry or HR department and the Data Protection Officer will liaise with the Head of Operations to access the necessary images in order to determine whether the processing is necessary for the prevention, investigation and detection of crime or the apprehension and prosecution of offenders and whether the request should therefore be complied with.

4.4.4. The Registry or HR department must ensure that a written acknowledgement is sent to the requestor as soon as practicable and in any event within 21 days of receiving the request containing the following:

- The name of the Data Subject.

- Either a confirmation that LSST will comply with the request to prevent processing of the CCTV images likely to cause substantial and unwarranted damage to the Data Subject or that LSST will not comply with the request to prevent processing of CCTV images likely to cause substantial and unwarranted damage to the Data Subject and the reasons for this decision or that no automated decision in respect of the CCTV images has been made by LSST.

4.5. Request from a Third Party for Access/Disclosure:

4.5.1. Unlike Data Subjects, third parties who wish to have access to, or a copy of, CCTV images (i.e., images not of the person making the request) do not have a right under the DPA to access, unless the exceptions below apply, and care must be taken when complying with such requests to ensure that neither the DPA nor the CCTV Code are breached. As noted above, requests from third parties will only be granted if the requestor falls within the following categories:

- Law enforcement agencies (where the images recorded would assist in a specific criminal case).

- Prosecution agencies (including School Managers undertaking Staff or Student disciplinary proceedings).

- Legal representatives of the Data Subject.

4.5.2. In order to ensure compliance with the DPA and the CCTV Code the following procedure must be complied with.

4.5.3. The third Party should be directed to LSST's Data Protection Officer.

4.5.4. The Third Party must be provided with a copy of the Third-Party Request Form attached as Annex C to enable them to make a formal request to view / receive copies of images, which they can either complete on site or take away and send it back.

4.5.5. The completed Third Party Request Form must then be given to the Head of Operations to pass on to the Registry or HR department and the Data Protection Officer.

4.5.6. The Registry or HR department and the Data Protection Officer will liaise with the Head of Operations in order access the requested images and in order to:

- Determine whether the request should be complied with.

- Ensure that the relevant images are located.

- Determine whether third party images (i.e., images of persons other than the intended Data Subject) are contained within the images.

- If applicable, ensure that any third-party images are disguised or blurred before access or disclosure is granted.

4.5.7. Once the images have been located and the Archives, Records and Information Access and the Head of Security have agreed that a Third-Party Request can be complied with, the Registry or HR department and the Data Protection Officer must provide the Third Party with written notice containing the following:

- The name of the Third Party.

- The date of receipt of the completed Third Party Request Form.

- A description of personal data (i.e., images of the Data Subject(s) recorded on the LSST CCTV system and dates when recorded).

- If the Third Party elected in their completed Third-Party Request Form to view the images at LSST, an invitation to contact the Registry or HR department and the Data Protection Officer to arrange a viewing of the images during normal business hours.

- If the Third Party elected in their completed Third-Party Request Form to receive a copy of the relevant images, references to a digital device being enclosed which contains the relevant images of the Data Subject with any third-party images blurred (if applicable).

4.5.8. If the Third Party views the images on LSST premises, an entry needs to be made in the CCTV Operating Log Book recording:

- The name(s) of the Third Party and any other attendees.

- The date and time of the viewing.

- The location where the viewing took place.

4.5.9. If the Registry or HR department and the Data Protection Officer determine that a Third-Party Request cannot be complied with, the Third Party must be provided with written notice containing the following:

- The name of the Third Party.

- The date of receipt of the completed Third Party Request Form.

- The reason for refusing to grant access to / supply the images requested (e.g., compliance with the request would, or would be likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, the images have already been erased etc.).

5. Disclosure to the Police

5.1. CCTV footage will be freely shared with the police to aid them in the pursuit of an investigation into criminal activity against the premises or personnel of LSST. In all cases an entry needs to be made in the CCTV Operating Log Book recording:

- The name of the Police Officer receiving a copy of the recording;

- Brief details of the images captured by the CCTV to be used in evidence;

- The crime reference number;

- Date and time the images were handed over to the Police.

5.2. Where information is requested by the police for the purposes of an investigation unrelated to criminal activity against the premises or personnel of LSST will only make such disclosures on receipt of a Section 29 Data Protection Act Form signed by a Senior Police (inspector or above) and once satisfied of the following:

- That the purposes are related to crime.
- That failure to release would prejudice the Police Investigation.

5.3. In all cases an entry needs to be made in the CCTV Operating Log Book:

- The name of the Police Officer receiving the copy of the recording.
- Brief details of the images captured by the CCTV to be used in evidence.
- The crime reference number.
- Date and time the images were handed over to the Police.

6. Monitoring Compliance with the DPA and the CCTV Code

6.1. An annual assessment will be undertaken by the Head of Operations, the Registry or HR department and the Data Protection Officer to evaluate the effectiveness of the CCTV system at LSST and its compliance with the DPA and the Code.

6.2. The results of the report will be assessed against the stated purpose of the system. If the system is not achieving its purpose, remedial action must be undertaken to modify the systems. Requests from members of the public for access to such reports will be considered by the Registry or HR department, and the Data Protection Officer on a case-by-case basis as per the requirements of the Freedom of Information Act.

7. Complaints Procedure

7.1. Complaints regarding the handling of the data by LSST should be lodged with the Information Commissioners Office (ICO) here: https://ico.org.uk/concerns/handling/ within 3 months of your last contact concerning the matter with the School (or such other time limit as the ICO may specify).

7.2. Complaints regarding the CCTV system and its operation should be made under the School's complaints procedure.

Annex A to Policy and Standards for CCTV Operation

Information Leaflet for the Operation of CCTV at LSST

This leaflet contains information and advice about the operation and management of the closed-circuit television (CCTV) system at LSST. It also provides information relating to your rights under the Data Protection Act 2018 (DPA).

Why do we have CCTV at LSST?

The purpose of the CCTV system is to enable the prevention, investigation and detection of crime, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), public, employee and student safety and monitoring the security of LSST premises.

How is it controlled?

The DPA provides a legal framework under which all personal data relating to individuals is processed, which extends to the recording of images on CCTV systems. The governmental authority that oversees and enforces the DPA, the Information Commissioner, has also issued a code of practice that specifically applies to CCTV (the CCTV Code). To ensure compliance with the DPA and the CCTV Code, LSST have introduced policies and procedures under which the CCTV system at LSST is to be operated. This Policy addresses issues such as who may have access to the monitoring and data storage equipment and contains guidelines for the operators to ensure that the individual's privacy is respected.

How does it operate?

The system is operated by LSST and monitored 24 hours a day, every day of the year. Images from the cameras are recorded and held for a minimum of 28 days. If there is no legitimate reason to keep the recording, the data is erased thereafter.

Who uses the images?

Access to the images recorded by the CCTV cameras is restricted and images can only be disclosed in accordance with the DPA and the CCTV Code. Persons who are not involved in the operation or supervision of the CCTV systems at LSST will only be granted access to, or disclosure of, the recorded images where such access or disclosure is necessary for the prevention, investigation and detection of crime, or the apprehension and prosecution of offenders. In every case LSST requires a written request to be made setting out the reason(s) for which the images are required. Normally disclosure will only be granted to the following third parties:

- Law enforcement agencies;
- Prosecution agencies; and
- Authorised legal representatives.

Can I see the images?

You are entitled to access personal information which is held about you by a third party, which extends to images of you recorded by the CCTV system at LSST. If you wish to exercise your right to see such images you will need to complete a Subject Access Request (SAR) form (see this policy further above regarding this). In order for us to be able to locate the relevant images on the SAR form you must be able to clearly identify yourself and the date, time and location in which you think you were recorded. Remember that images will ordinarily be erased after 28 days. LSST will respond within 40 days of receiving the required information and search fee either identifying the steps taken to comply with the request or setting out the reasons for refusing the request.

How do I make a complaint?

Complaints regarding the handling of the data by LSST should be lodged with the Information Commissioners Office (ICO) here: https://ico.org.uk/concerns/handling/ within 3 months of your last contact concerning the matter with the School (or such other time limit as the ICO may specify).

Is LSST's CCTV effective?

CCTV has a wide range of uses and is part of a number of initiatives LSST uses to ensure the safety and security of our premises and of the people accessing them.

Annex B to Policy and Standards for CCTV Operation

DATA PROTECTION ACT 2018 –
SUBJECT ACCESS REQUEST FORM
CCTV AT LSST

(*Please use BLOCK CAPITALS to complete this Form*)

The Data Protection Act 2018 (DPA) provides Data Subjects (individuals to whom "personal data" relates) with a right to access personal data held about themselves, including images recorded on closed circuit television (CCTV) systems.

To enable LSST to deal promptly with your request for access to CCTV images, please complete this form, giving as much information as possible to help us identify the requested data.

Under the terms of the DPA, LSST has 30 days to comply with your request. This time period will ordinarily commence on the date that your completed form and/ or any further necessary information is received by LSST to enable LSST to respond to your request.

1. PERSONAL DETAILS OF THE DATA SUBJECT

Title Surname

First Name(s)

Date of Birth __ __ __ Male / Female

Permanent Residential Address

Post Code

Daytime Telephone Number

2. INFORMATION REQUIRED TO LOCATE IMAGES

In order for LSST to identify the images you require access to, please provide the following information:

The exact date(s), time(s) and location(s) of the CCTV system camera(s) which captured the footage required:

.....

.....

Sufficient personal characteristics to enable identification of the Data Subject (a full description including hair colour, clothing etc.) together with a photograph. Please use a separate sheet of paper if necessary:

.....

.....

3. ACCESS TO IMAGES

Assuming LSST is able to locate the required images, please select (*X*) which of the following will satisfy your request:

I would like to view the relevant images at LSST

I would like to be sent a copy of the relevant images

4. REASON WHY YOU ARE REQUESTING THE CCTV IMAGES

.....

.....

.....

.....

5. ACKNOWLEDGEMENT

I acknowledge that it may be necessary for LSST to contact me in order to obtain further information in order to be satisfied as to my identity or to locate my personal data.

I acknowledge that if LSST is of the opinion that complying with this request would, or would be likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, LSST has the right under the DPA to decline this request.

Signature Date __

Return this form to:

Data Protection Officer
London School of Science & Technology
Memo House
1st Floor, Kendal Ave.
London
W3 0XA

Or by email at legal@lsst.ac

Annex C to Policy and Standards CCTV Operation

DATA PROTECTION ACT 2018
THIRD PARTY REQUEST FORM
CCTV AT LSST

(*Please use BLOCK CAPITALS to complete this Form*)

The Data Protection Act 2018 (DPA) regulates the processing of personal data relating to Data Subjects (individuals to whom "personal data" relates), including images recorded on closed circuit television (CCTV) systems.

Access to the images recorded by the CCTV cameras is restricted and images can only be disclosed in accordance with the DPA and the code of practice issued by the governmental authority that oversees and enforces the DPA, the Information Commissioner that specifically applies to CCTV (the CCTV Code). Persons who are not involved in the operation or supervision of the CCTV systems at LSST will only be granted access to, or disclosure of, the recorded images where such access or disclosure is necessary for the prevention, investigation and detection of crime, or the apprehension and prosecution of offenders.

1. DETAILS OF THE THIRD-PARTY APPLICANT

Title Surname

First Name(s)

Incident Number (if applicable)

Organisation Name

Organisation Address

Post Code

Daytime Telephone Number

Please select (*X*) which of the following types of organisation you are applying on behalf of:

☐ Law enforcement agency

☐ Prosecution agency

Legal representative – please state whom you represent ……...

Other (please Specify)

…….....

2. PERSONAL DETAILS OF THE DATA SUBJECT (IF APPLICABLE)

Title Surname

First Name(s)

Date of Birth __ __ __ Male / Female

3. INFORMATION REQUIRED TO LOCATE IMAGES

In order for LSST to identify the images you require access to, please provide the following information:

The date, time and location of the CCTV systems camera which captured the footage required:

.....

.....

Sufficient personal characteristics to enable identification of the Data Subject (if applicable) include a full description including hair colour, clothing etc together with a photograph (if possible). Please use a separate sheet of paper if necessary:

.....

.....

.....

4. ACCESS TO IMAGES

Assuming LSST is able to locate the required images, please select (*X*) which of the following will satisfy your request:

I would like to view the relevant images at LSST

I would like to be sent a copy of the relevant images

6. REASON WHY YOU ARE REQUESTING THE CCTV IMAGES

.....

……

……

……

6. ACKNOWLEDGEMENT

I acknowledge that it may be necessary for LSS Try to contact me in order to obtain further information in order to be satisfied as to my identity or to locate the requested images.

I acknowledge that LSST has the absolute discretion to determine whether a request for access to, or disclosure of, the images recorded on the CCTV systems at LSST is necessary for the prevention, investigation and detection of crime, or the apprehension and prosecution of offenders.

I acknowledge that if LSST is of the opinion that complying with this request would, or would be likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, LSST has the right decline this request.

Signature Date ____/ ___/ _____

Version History

Version	**1.0 – 4.0**	
Original author(s):	Head of Security Head of Operations	
Reviewed by:	Executive Committee	September 2016 September 2017 September 2018 September 2019
Version	**4.1**	
Revised by:	Quality Unit Head of Operations	
Revision summary:	*Annual review and update; Formatting and version control applied.*	
Reviewed by:	Board of Governors	October 2020
Version	**4.2**	
Revised by:	Quality Unit Head of Operations	
Revision summary:	*Annual review and update.*	
Approved by:	Board of Governors	October 2021
Version	**4.3**	
Revised by:	Quality Unit Senior Operations Manager	
Revision summary:	*Annual review and update; minor grammatical changes.*	
Approved by:	Board of Governors	November 2022
Version	**5**	
Revised by:	Quality Unit Senior Operations Manager	
Revision summary:	*Annual review; version control applied*	
Approved by:	Board of Governors	October 2023
Version	**6**	
Revised by:	Quality Unit Head of Operations	
Revision summary:	*Annual review and update, minor grammatical corrections, document format applied, version control applied.*	
Approved by:	Board of Governors	October 2024
Version	**7.0**	
Original author(s):	Head of Security Head of Operations	
Revised by:	Quality Unit Head of Operations	
Revision summary:	*Annual review and update -* *Minor grammatical corrections, document format applied, version control applied.*	
Reviewed by: Approved by:	Publications Committee Board of Governors	September 2025 October 2025

Version	7.1	
Original author(s):	Head of Security Head of Operations	
Revised by:	Quality Unit Head of Operations	
Revision summary:	*UK GDPR and Data Protection Act 2018 referenced throughout document to reflect updated legislation. Points 4.3.5, 4.3.6, and 4.3.7 added on the Subject Access Request process. Principal, Deputy CEO, and General Counsel changed to Registry or HR department and Data Protection Officer throughout document to reflect current processes.*	
Reviewed by:	Publications Committee	February 2026
Approved by:	Board of Governors	February 2026