1. Introduction

1.1 A Closed Circuit Television (CCTV) system (‘the System’) is in use at all British Library sites, both in public areas and also in certain staff areas with specific security requirements. The System comprises a number of cameras installed at strategic locations, the images from which are presented in our Security Control Rooms at St Pancras and Boston Spa. The images are generated by cameras working in both the visible and non-visible sections of the electromagnetic spectrum.

1.2 For the purposes of the Data Protection Act 2018, the ‘Data Controller’ of the System is the British Library Board. The Board considers that the use of CCTV by the British Library is a necessary, proportionate and suitable tool to help reduce crime, protect the public and staff, and to assist with maintaining the security of the Library’s assets; these actions form part of the Library’s public task, as set out in the British Library Act 1972.

2. Purpose & Objectives

2.1 The System is operated solely for the purposes of safety and security, including the prevention and detection of crime.

2.2 The specific objectives of the System, as determined by the British Library Board, are to:

- Enhance the safety and security of visitors and staff
- Assist the Library in maintaining the security and protection of its assets, and in particular, the national Collections
- Help reduce crime, disorder, and fear of crime
- Deter those having criminal intent
- Aid in the detection of crime
- Give confidence to staff, contractors and visitors that they are in a secure environment
- Provide management information relating to Health and Safety matters and the management of emergencies on British Library sites.
- Gathering evidence to support these purposes
3. **Responsibilities**

3.1 **System Owner** – The British Library Board is the ‘owner’ of the System. The **Head of Safety & Security** is the Board’s delegated representative in relation to the System, and has unrestricted access to the CCTV Control Room(s). The delegated representative of the System Owner is responsible for:

- Maintaining a close liaison with Security Operations Managers
- Ensuring the interests of the British Library Board in relation to the operation of the System
- Authorising any proposed alterations to the System and/or its associated procedures.

3.2 **System Manager** - The **Head of Security Operations** manages the System on behalf of the System Owner on a day to day basis, and is responsible for:

- Day to day management of the System and its operating staff
- Ensuring that this policy is complied with during the operation of the System
- Ensuring the security of the Library’s CCTV Control Room(s)
- Liaising with the System Owner’s delegated representative, and ensuring they are aware of any issues relating to the operation of the System
- Liaising with internal stakeholders in relation to the operation of the System
- Investigation of any complaints made in relation to the operation of the System (with the advice of the Data Protection Officer as appropriate).

3.3 **Systems Maintenance** – The **Technical Security Manager** is responsible for:

- Ensuring the provision and maintenance of all equipment forming part of the System, as specified or authorised by the System Owner.

3.4 **Data Protection Officer** – The Library’s statutory **Data Protection Officer** has unrestricted access to the CCTV Control Room(s) and is responsible for:

- Advising on Data Protection Impact Assessments in relation to changes to the location or operation of CCTV cameras
- Advising on requests for access to or copies of CCTV footage
- Biennial audit of the System in relation to Data Protection compliance.

4. **Data Protection**

4.1 The processing of all personal data gathered by the System will be managed strictly in accordance with the requirements of the Data Protection Act 2018.
4.2 The processing of all personal data gathered by the System will be managed in accordance with the Library’s published Privacy Policy.

4.3 The System components that directly carry out surveillance activities (such as cameras and sensors) must not be moved, re-pointed, replaced, or added to, unless a Data Protection Impact Assessment has first been completed and authorised, in accordance with normal Library processes as published on the Library Intranet.

4.4 Requests for personal data held by the Library by virtue of the operation of the System shall be managed as set out in Section 9 of this policy.

5. General Principles

5.1 The Library will voluntarily comply with the 12 Guiding Principles set out in the Code of Practice published by the Surveillance Camera Commissioner. This policy sets out the means by which it will do so.

5.2 The System will be operated fairly, within the law, and only for the purposes for which it was established as identified within this policy.

5.3 Throughout this policy it is intended, as far as reasonably possible, to balance the Library’s objectives for the System with the need to safeguard the rights of individuals.

5.4 The areas covered by CCTV to which this policy refers are the premises operated by and/or on behalf of the British Library Board and those public areas around the perimeter of such premises.

5.5 Any major changes to this policy that would have a significant impact upon either the operation of the system or the privacy of staff and visitors will take place only after consultation with all relevant stakeholders, including the Library’s Trade Unions. Minor changes that do not have a significant impact upon either the operation of the system or the privacy of staff or visitors may be agreed between the Representative of the System Owner, the Senior Information Risk Owner (SIRO), and the Data Protection Officer.

6. CCTV Control Room(s)

6.1 A Control Room, staffed 24/7, is located at The British Library, 96 Euston Road, London NW1 2DB. The CCTV equipment in use has the capability of recording all Library cameras simultaneously throughout every 24 hour period.
6.2 Secondary Control Rooms are located at The British Library, Boston Spa, Yorkshire, and in the basement of our St Pancras building.

6.3 Passive body scanning functionality is operated from a dedicated control area on the Lower Ground Floor of our St Pancras building. The System has the capability of recording images generated by this functionality but does not routinely make such records.

6.4 Access to the Library’s CCTV Control Room(s) is restricted to authorised personnel only, for reasons of security and confidentiality.

6.5 The level of staffing required in Control Room(s) will be determined in accordance with Library operational procedures.

6.6 Every person involved in the management and operation of the system will be personally issued with a copy of this policy and any associated operational procedures. They will be required to sign a contractual confirmation that they fully understand the obligations that adherence to this document places upon them and that any breach may be considered as a disciplinary offence (See Annex A). They will be fully conversant with the contents of this policy (as may be updated from time to time) and will be expected at all times to comply with it, insofar as is reasonably practicable.

6.7 All personnel involved with the System shall receive training from time to time covering all legislation relevant to the operation of the System, including Data Protection law and Known Consignor regulations. All personnel involved with the System shall maintain any relevant licences and qualifications as may reasonably be requested by the Library, including SIA licences and Known Consignor clearances.

6.8 Every individual with any responsibility under this policy or who has any involvement with the System to which it refers is subject to the British Library Disciplinary Policy. Misuse of the System, or any breach of confidentiality relating to the operation of the System, may constitute gross misconduct under the Disciplinary Policy, and may also constitute a criminal offence under section 170 of the Data Protection Act 2018.

6.9 The System Manager has day to day responsibility for the security and management of the Control Room(s), and for enforcing the operation of this policy and any associated operating procedures.

6.10 Access to the Control Room(s) by any party other than authorised staff and those named in this policy is prohibited, except on the personal authority of the System Manager (or their nominated deputy) for lawful and proper reasons.

6.11 Visits by properly authorised inspectors or auditors do not fall into the scope of the above paragraph and may take place at any time, without prior warning, and without the authorisation of the System Manager. Any visit for these purposes will be suspended in the event of it becoming operationally necessary.
6.12 All access to the Control room(s) by any person other than the Representative of the System Owner, the System Manager (or their nominated deputy), and/or rostered Control Room Staff must be recorded in the Daily Occurrence Book. All such visitors must also sign the Visitors Book to acknowledge their understanding of the associated confidentiality requirements. See Annex B for signage.

6.13 At least one member of authorised personnel should be in attendance at the Control Room(s) at all times when the System is in use. If a working Control Room is left unattended for operational reasons (for example, an evacuation for safety reasons) then it must be secured.

6.14 Control Room(s) should at all times be secured by access control equipment such as magnetic locks or other equally secure means.

7. **Operation of Cameras**

7.1 Any person operating the cameras must act with the utmost probity at all times.

7.2 Only those trained and authorised members of staff with responsibility for using the CCTV equipment are permitted to operate any equipment associated with the System.

7.3 Every use of the cameras made by those operators must be in accordance with the purposes of the System and must be in compliance with this Policy.

7.4 Cameras must not be used to look into private residential property. Where possible, the System shall be configured to prevent this.

7.5 Operators may be required at any time to justify to the System Manager their interest in, or recording of, any particular individual, group of individuals, or property. Camera operators must be mindful of the appearance of prejudice, which may lead to complaints that the system is being used for purposes other than those for which it is intended.

8. **Maintenance of Cameras**

8.1 To ensure compliance with the Data Protection Act 2018 and that images recorded continue to be of appropriate evidential quality, the System must be regularly maintained to a standard specified by the Representative of the System Owner. This standard should be written in to a maintenance agreement with any relevant supplier contracted for such a purpose.
8.2 The Technical Security Manager will make provision for regular / periodic service checks on the equipment comprising the System, which will include cleaning of any weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

8.3 The System Owner must make provision to allow the Technical Security Manager to undertake regular periodic overhaul of all the equipment comprising the System and/or the replacement of equipment which is reaching the end of its serviceable life.

8.4 Any maintenance agreement must provide for ‘emergency’ attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control, and should define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

8.5 The System Manager is responsible for ensuring that appropriate records are maintained in respect of the functioning of the cameras.

9. Requests for Recorded Material

9.1 General

9.1.1 For the purposes of this policy, ‘recorded material’ means any material recorded by (or as the result of) technical equipment which forms part of the System, and specifically includes CCTV footage, and static images extracted from such footage.

9.1.2 Every recording obtained by using the System has the potential to contain material that may need to be admitted as evidence at some point during its life span.

9.1.3 Everyone must have total confidence that information recorded by the System about their ordinary activities will be treated with due regard to their individual right to respect for their private and family life or other rights to privacy. It is therefore of the utmost importance that all data obtained from, or used in conjunction with, the System are treated strictly in accordance with this policy and any associated operational procedures.

9.1.4 Recorded material must never be copied, sold, released, or otherwise used for commercial purposes or for the provision of entertainment.

9.1.5 Access to, or the provision of copies of, recorded material may not be provided to any person except as part of the processes defined in the rest of Section 9 of this policy.
9.2 Routine use of CCTV for Security or Health & Safety Purposes

9.2.1 The authorised operators of the System monitor the Library’s premises for the purposes of security and health & safety, and take actions (such as alerting other security officers) based on information observed. Authorised operators are permitted to repoint PTZ cameras at their discretion in order to support these purposes (for example, to focus on a specific area, group, or individual of interest).

9.2.2 The System routinely records footage from all operational cameras, which is retained for a period of 31 days before being overwritten, unless specific action is taken to preserve the footage for a longer period.

9.2.3 The Control Room Security Manager or Security Manager BSP (or their authorised deputies) may authorise the retention of CCTV footage for a longer period where there is a reasonable belief that such footage may be needed as evidence in relation to a security or health & safety incident. The Security Team Manager on duty at the time of the incident should inform the appropriate line manager of any incident where they believe that this may become the case. The details of the retained footage, including the reason for which it has been retained, must be recorded in the Daily Occurrence Book.

9.2.4 Recorded material may be used for staff training purposes at the discretion of the System Manager.

9.3 Extract of Recorded Material for Security or Health & Safety Purposes

9.3.1 A digital print or other extract of recorded material from the System may occasionally be required for operational security purposes (for example, to alert front-of-house staff to a potential threat). In these circumstances the Control Room Security Manager or Security Manager BSP should consult with the Data Protection Officer in the first instance.

9.3.2 Assuming that both parties are agreed that the distribution of the recorded material in question is justified, targeted, and proportionate then the relevant security manager may authorise the extraction and circulation of the recorded material.

9.3.3 The details of the extracted footage or digital print, including the reason for which it was extracted, must be recorded in the Daily Occurrence Book.

9.3.4 Recipients of the recorded material must be informed of the need to keep the recorded material confidential and secure.

9.3.5 The relevant security manager should put in place measures to ensure that the recorded material is securely disposed of once the operational requirement has passed.
9.4 **Internal Investigations**

9.4.1 On occasion the People Team (or Fraud Response Team or other authorised persons) may need to view recorded material (or be provided with a copy of such material) as part of the legitimate performance of their duties. Such duties might include, for example, the investigation of allegations of criminal activity or serious breaches of health & safety.

9.4.2 All such requests must be authorised by the process set out in the Digital Investigation Policy.

9.4.3 Authorised operators of the System must not action such requests without proof of authorisation from both the Data Protection Officer and either the Head of People or one of the Chief Officers.

9.4.4 The details of the extracted footage or digital print, including the reason for which it was extracted, must be recorded in the Daily Occurrence Book.

9.4.5 Recipients of the recorded material must be informed of the need to keep the recorded material confidential and secure.

9.5 **Subject Access Request**

9.5.1 Under the Data Protection Act 2018, any individual has the right to request a copy of any recorded material that records them.

9.5.2 Normally such requests will be received directly by the Data Protection Officer. Should such a request be received directly by a member of the Security Team they should either forward it to the Data Protection Officer at dp@bl.uk (if the request has been received in writing), or direct the requestor to put their request in writing to that address (if the request has been made orally).

9.5.3 Authorised operators of the System must not action such requests except on the instruction of the Data Protection Officer. Authorised operators of the System must not provide recorded material directly to the recipient.

9.5.4 The details of the extracted footage or digital print, including the reason for which it was extracted, must be recorded in the Daily Occurrence Book.

9.5.5 The Data Protection Officer is responsible for providing the recorded material to the requestor in secure fashion, and advising them of any legal responsibilities that they may have in relation to the recorded material.
9.6 Police Request – Operational Emergency

9.6.1 Under the Regulation of Investigatory Powers Act, the Police may request that the Library cooperate in surveillance activities in immediate response to an unfolding situation (for example, a terrorist threat or similar emergency).

9.6.2 Normally such a request must be made by a police officer of Inspector or higher rank. For the Library’s part, such cooperation must be authorised by the Control Room Security Manager or Security Manager BSP or higher if present, or by the duty Security Team Manager if not.

9.6.3 If such cooperation is authorised, relevant police officers may be invited into the Control Room in order to direct the urgent surveillance activity in question.

9.6.4 The presence of the police officers, the reason for the operation, the persons authorising the surveillance on both side, and all other relevant details must be recorded in the Daily Occurrence Book.

9.7 Police Request – Planned Surveillance

9.7.1 Under the Regulation of Investigatory Powers Act, the Police may request that the Library cooperate in planned and potentially long running surveillance activities for the purpose of protecting national security, preventing or detecting crime, or in the interests of public safety or health.

9.7.2 Normally such a request must be made in writing by a police officer of Superintendant or higher rank. For the Library’s part, such cooperation must be authorised by the System Manager or the Representative of the System Owner.

9.7.3 If such cooperation is authorised, relevant police officers may be invited into the Control Room in order to direct the surveillance activity in question.

9.7.4 The presence of the police officers, the reason for the operation, the persons authorising the surveillance on both side, and all other relevant details must be recorded in the Daily Occurrence Book.

9.8 Police Request – Investigation

9.8.1 A police officer conducting an investigation into a crime may request to view (or to receive a copy of) recorded information.

9.8.2 Normally such requests will be received directly by the Data Protection Officer. Should such a request be received directly by a member of the Security Team they should either forward
it to the Data Protection Officer at dp@bl.uk (if the request has been received in writing), or
direct the requesting police officer to put their request in writing to that address (if the
request has been made orally).

9.8.3 Authorised operators of the System must not action such requests except on the instruction
of the Data Protection Officer. Authorised operators of the System must not provide
recorded material directly to the requesting police officer.

9.8.4 The details of the extracted footage or digital print, including the reason for which it was
extracted, must be recorded in the Daily Occurrence Book.

9.8.5 The Data Protection Officer is responsible for providing the recorded material to the
requesting police officer in secure fashion, and advising them of any legal responsibilities
that they may have in relation to the recorded material.

9.9 Third Party Request

9.9.1 Occasionally a third party may request to view (or to receive a copy of) recorded information
(for example, an insurer wishing to view footage of a road traffic accident outside of the
Library, an inquiry seeking evidence, a solicitor requesting disclosure of evidence, or a
journalist seeking information via a Freedom of Information request).

9.9.2 Normally such requests will be received directly by the Data Protection Officer. Should such
a request be received directly by a member of the Security Team they should either forward
it to the Data Protection Officer at dp@bl.uk (if the request has been received in writing), or
direct the requestor to put their request in writing to that address (if the request has been
made orally).

9.9.3 Authorised operators of the System must not action such requests except on the instruction
of the Data Protection Officer. Authorised operators of the System must not provide
recorded material directly to the requestor.

9.9.4 The details of the extracted footage or digital print, including the reason for which it was
extracted, must be recorded in the Daily Occurrence Book.

9.9.5 The Data Protection Officer is responsible for providing the recorded material to the
requestor in secure fashion, and advising them of any legal responsibilities that they may
have in relation to the recorded material.

10. Signage and Transparency Obligations

10.1 The Library is obliged to inform persons who may be recorded by the System of its existence,
and how they might receive more information about its operation.
10.2 Clear signage must be maintained at all points where members of public may enter the area under surveillance by the System (e.g. at all points of access to the Library’s estate). It is also good practice to include such signage at points of entry into buildings. Such signage should clearly indicate that surveillance is being undertaken for the purposes of security and health & safety, and provide contact details for the System Owner and/or the Data Protection Officer.

10.3 All additional details required to comply with the Transparency requirements of the Data Protection Act should be made available via the Library’s Privacy Policy and Transparency Notices.

11. Complaints

11.1 A member of the public wishing to register a complaint with regard to any aspect of the System may do so by contacting the System Manager. The System Manager will liaise with the Library’s Data Protection Officer in order to establish the correct Library process for investigating the complaint (which will normally be the Data Protection complaints process), and will ensure that every complaint is acknowledged in writing within five working days. The acknowledgment will include advice to the complainant of the enquiry procedure to be undertaken. A formal investigation of the complaint should be undertaken by the System Manager, and a written report is be forwarded to the Representative of the System Owner within seven working days. The report should contain details of the complaint and the outcome of relevant enquiries. The Representative of the System Owner will then direct the System Manager as to how to respond to the complaint, and any additional remedial actions that must be taken.

12. Assessment

12.1 Every two years the System Manager shall evaluate the System to establish whether the purposes of the System are being complied with and whether its objectives are being achieved. A report of the evaluation must be provided to the Representative of the System Owner and the Corporate Information Governance Group, and must include:

i) An assessment of the incidents monitored by the system in the past 24 months

ii) An assessment of the impact on crime

iii) The operation of this policy

iv) Whether the purposes for which the system was established are still relevant

v) Cost effectiveness
vi) Recommendations for improvement (if any).

12.2 Following receipt of the report, the Data Protection Officer shall review this policy and recommend any necessary amendments to the Representative of the System Owner and the Senior Information Risk Owner at the next meeting of the Corporate Information Governance Group.

12.3 The Data Protection Officer (or his/her nominated deputy who is not the System Manager) is responsible for auditing the operation of the System, the records of data processing activity relating to each camera, and compliance with this policy on a biennial basis.
Annex A:

Declaration of Confidentiality

The British Library CCTV System

I, .............................................., am retained by the British Library to perform the duty of
............................................................................................ I have received a copy of the British Library CCTV Policy
in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of the British Library CCTV Policy and understand that
all duties which I undertake in connection with the British Library System must not
contravene any part of the current Policy, or any future amendments of which I am made
aware.

If now, or in the future, I am or become unclear of any aspect of the operation of the System
or the content of the CCTV Policy, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any
individual, firm, company, authority, agency or other organisation, any information which I
may have acquired in the course of, or for the purposes of, my position in connection with
the CCTV System, verbally, in writing or by any other media, now or in the future, (including
such time as I may no longer be retained in connection with the CCTV System), unless
properly authorised to do so.

In appending my signature to this declaration, I agree to abide by the British Library CCTV
Policy at all times. I also understand and agree to maintain confidentiality in respect of all
information gained during the course of my duties, whether received verbally, in writing or
any other media format - now or in the future.

I further acknowledge that I have been informed and clearly understand that the
communication, either verbally, in writing or by any other means including, for example, e-
mail, to any unauthorised person(s) of any information acquired as a result of my
employment with the British Library may be an offence against the British Library Conduct
and Disciplinary Policies.

Signed: .............................................. Print Name: ..............................................

Witness: .............................................. Position: ..............................................

Dated this .............................. day of .............................................. (Month) 20.....
Annex B:

**Restricted Access Notice**

**RESTRICTED ACCESS AREA**

Everyone other than authorised members of Control Room staff who enters this area is required to complete an entry in the Visitors Book.

Visitors must note the following confidentiality clause. Entry is conditional on acceptance of that clause:

**Confidentiality Clause:**

‘In being permitted entry to this area you agree not to divulge any information obtained, overheard or overseen during your visit. An entry accompanied by your signature in the Visitors book is your acceptance of these terms.’