Northern Ireland Assembly

Parliament Buildings CCTV Policy

October 2018 - V 1.6

Contents

Introduction and Objectives

1.1 Introduction

The Northern Ireland Assembly Commission's (hereafter referred to as the Commission) Parliament Buildings CCTV policy is based upon the *Information Commissioners Data Protection Code of Practice for Surveillance Cameras and Personal Information*, and adheres to the 12 guiding principles outlined within that Code of Practice. The policy also takes into consideration the *Surveillance Commissioner's Code of Practice*

The Commission operates a CCTV system for Parliament Buildings which is located within the Stormont Estate, Belfast. Images are monitored and recorded centrally, and are used in strict accordance with CCTV policy and the aforementioned Codes of Practice.

The CCTV System is owned by the Northern Ireland Assembly Commission (NIAC), Parliament Buildings, Ballymiscaw, Stormont, Belfast BT4 3XX, and is managed and controlled from the Assembly Control Room within Parliament Buildings. All locations that are covered by the CCTV system fall within this policy.

The CCTV System comprises a number of CCTV cameras, located at strategic points, principally at the entrances of Parliament Buildings and within the building itself. A number of CCTV cameras are also located outside Parliament Buildings albeit within its immediate environs. These cameras allow the Commission to carry out surveillance of selected interior and exterior areas of Parliament Buildings.

The Head of Usher Services with the support of designated staff, has overall responsibility for the operation of the CCTV System, and for ensuring compliance with this policy and the procedures documented in the CCTV Operational Procedures Manual.

Contact details are as follows:

Head of Usher Services	Ken Eccles (02890) 521945 Ext 21945 Email: ken.eccles@niassembly.gov.uk
or in his absence	Marc McLaughlin (02890) 521626 Ext 21626 Email: Marc.McLaughlin@niassembly.gov.uk
or	Stephen.Scott (02890) 521006 Ext 21006 Email: Stephen.Scott@niassembly.gov.uk

The CCTV System is primarily comprised of CCTV cameras both fixed and Pan, Tilt, Zoom (PTZ), video monitors, multiplexers, digital recorders and signage.

Signs are prominently placed at strategic locations including entrances to Parliament Buildings, to inform staff, Members, visitors and members of the public that a CCTV installation is in use and to provide details of whom to contact about the system.

Details of the CCTV System have been provided to the Information Commissioner, and will be reviewed and updated annually as appropriate.

1.2 Definitions

Data Controller	The Northern Ireland Assembly Commission (NIAC)
System Manager	The Head of Usher Services.
System Owner	The Northern Ireland Assembly Commission (NIAC)

Details of key personnel, their responsibilities and contact points are shown at Appendix (A) of this document.

1.3 Statement in Respect of the Human Rights Act 1998

The Commission recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998.

The Commission considers that the use of CCTV is a necessary, proportionate and suitable means to primarily prevent, detect and help reduce criminal activity which may pose a threat to NIA business and all those frequenting Parliament Buildings. The secondary function of the CCTV system is to assist with public safety.

The CCTV System will be operated with respect for all individuals, recognising their right to be free from inhuman or degrading treatment, and will avoid discriminating on any grounds such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

The CCTV System will also be operated in such a way as to avoid any infringement of individual privacy, and this will be reflected within the Data Privacy Impact Assessment (DPIA) notices.

The Commission recognises its responsibility to ensure that the CCTV System should always comply with all relevant legislation to ensure its legality, legitimacy and fitness for purpose.

The CCTV System will be used reactively only as a proportionate response to identified problems, and then only in so far as it is both reasonable and necessary in a democratic society:

- in the interests of national security and public safety,
- for the prevention and detection of crime or disorder,
- for the protection of health and
- for the protection of the rights and freedoms of others.

Adherence to ICO Code of Practice, Commission CCTV policy and CCTV Operational Procedures shall ensure that evidence is secured, retained and made available as required by law, so that there is at all times an absolute respect for individuals' rights.

1.4 Objectives of the CCTV System

The CCTV System has been installed by the Commission to protect Parliament Buildings and help ensure the safety and security of all building users, consistent with respect for individual privacy. These objectives will be achieved by the appropriate management and proper operation of the CCTV System.

The Commission's notification to the Information Commissioner states the purpose of the CCTV system is primarily for:

- Crime prevention and detection, and the apprehension and prosecution of offenders
- Deterring those persons with criminal intent;
- Assisting in the prevention and detection of crime;
- Facilitating the identification, apprehension and prosecution of offenders in relation to crime and public order;
- Facilitating the movement of vehicles on site;

The CCTV System will not be used:

- To provide recorded images for the world-wide-web;
- For any automated decision taking.

1.5 Procedural Manual

A CCTV Operational Procedures Manual has been produced which offers instructions on all aspects of the day to day operation of the CCTV System.

1.6 Monitor and Review

The operation of the CCTV System is monitored on a daily basis by line management and supervisors using specifically designated PCs in rooms B28 and B35, and is maintained on a quarterly basis by the main contractor/supplier. That maintenance programme is overseen and managed by Head of Building Services.

Statement of Purpose and Principles

2.1 Purpose

The purpose of this document is to set out the intended use of the CCTV System within the objectives outlined in Section (1).

2.2 General Principles of Operation

The CCTV System will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

The operation of the CCTV System also recognises the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000.

The CCTV System will at all times be operated fairly, within both the law and the provisions of the General Data Protection Regulation 2018. It will be used only for the purposes already outlined.

Public interest and confidence in the operation of the CCTV System will be safeguarded by ensuring the security and integrity of all operational procedures.

Structures for the management and operation of the CCTV System have been put in place, as has a procedure to deal with complaints received regarding the operation of the system.

2.3 Copyright

Copyright and ownership of all material recorded by virtue of the CCTV system will remain with the Data Controller.

2.4 Cameras and Area Coverage

The areas covered by the CCTV System are those specific locations within Parliament Buildings and its immediate external environs.

CCTV cameras are located at strategic points, principally at entrances and site entry/exit points.

All cameras are overt and visible, and none are hidden from view.

Cameras normally offer full colour, but may automatically switch to monochrome in low light conditions.

2.5 Monitoring and Recording Facilities

The CCTV System cameras will be operated and monitored on a 24 hour, 365 day basis from the Assembly Control Room. The CCTV System also has the capability of recording throughout any 24hour period.

All cameras can be monitored at any time on either a random or selected basis. Duplicate monitoring and recording facilities also exist within the Assembly Control Room.

The CCTV System is able to record images from selected cameras in real-time, produce hard copies of recorded images, and replay or copy any pre-recorded data in accordance with the policy. All viewing and recording equipment will be operated by appropriately trained and authorised users.

2.6 Human Resources

Unauthorised access to the Assembly Control Room is not permitted at any time. Access is strictly limited to those Control Room Operators on duty, Usher Services management, other specified Assembly senior management, PSNI and any other persons with a statutory power of entry upon production of written authority. A list of those members of management authorised to access the Assembly Control Room is shown at Appendix A of this document.

All Control Room Operators shall receive training relevant to their role and in accordance with procedure. This will include refresher training as necessary.

2.7 Processing and Handling of Recorded Material

All recorded material will be processed and handled strictly in accordance with this policy and the Operational Procedures Manual.

2.8 Operators Instructions

Technical instructions on the use of the CCTV System equipment are contained in the aforementioned Operational Procedures Manual provided by the equipment suppliers, a copy of which will be retained in Room B35.

2.9 Changes to the Code or the Procedural Manual

Any major changes to either the policy or the Operational Procedures Manual, will take place only after consultation with the CCTV System Manager.

Privacy and Data Protection

3.1 Public Concern

All personal data obtained by virtue of the CCTV System, shall be processed fairly and lawfully, and in particular only in the exercise of achieving the stated objectives of the CCTV System.

In processing personal data, a person's right to respect for his or her private and family life, will always be observed. (see paragraph 2.2)

The processing, storage and security of the data will be strictly in accordance with the requirements of the General Data Protection Regulation 2018 and additional locally agreed procedures.

Where the equipment permits, 'Privacy Zones' will be programmed into the CCTV System as required.

3.2 Data Protection Legislation

The operation of the CCTV System has been notified to the Office of the Information Commissioner, in accordance with current regulation

The Head of Usher Services has overall managerial responsibility for the CCTV System, though day to day responsibility for data management has been devolved to the Principal Ushers.

All data will be processed in accordance with the principles of the General Data Protection Regulation 2018, summarised as outlined:

- All personal data will be processed fairly and lawfully.
- Personal data will be obtained only for the purposes specified.
- Personal data held will be adequate, relevant and not excessive in relation to the purpose for which the data is processed.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Personal data will be processed in accordance with individuals' rights.
- Procedures will be in place to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.
- Information shall not be transferred outside the European Economic Area unless the rights of individuals are protected.

3.3 Request for information (subject access)

Any request from an individual for the disclosure of personal data which is believed to have been recorded by virtue of the CCTV System will be directed in the first instance to the Head of Usher Services.

The principles of the General Data Protection Regulation 2018 shall be followed in respect of every such request.

If the request cannot be agreed without identifying another individual, permission from that individual must be obtained unless it is reasonable in all the circumstances to comply with the request without the consent of that individual.

Any person making a request must be able to satisfactorily prove their identity, and provide sufficient information to enable the data to be located.

3.4 Exemptions to the Provision of Information

In considering a request made under legislative provision, reference may also be made to that legislation which includes, but is not limited to the following:

Personal data processed for any of the following purposes –

- the prevention or detection of crime
- the apprehension or prosecution of offenders

These are exempt from the subject access provisions in any case, to the extent to which the application of those provisions to the data subject would be likely to prejudice the matters referred to above.

Accountability and Public Information

4.1 The Public

Access to the Assembly Control Room is restricted in accordance with this policy (see Appendix A). However, in the interest of openness and accountability, anyone wishing to visit the Assembly Control Room may be permitted to do so, subject to the privacy considerations of others, and also with the prior approval of the CCTV System Manager (Head of Usher Services) or Director of Corporate Services.

Any complaints with regard to any aspect of the CCTV System should be addressed in the first instance to the Head of Usher Services – contact details are as follows:

Ken Eccles
Head of Usher Services,
NI Assembly, Parliament Buildings, Ballymiscaw, Stormont, Belfast, BT4 3XX
Tel: (028) 90521945 (Ext 21945)
Email: ken.eccles@niassembly.gov.uk

Concerns or enquiries relating to the provisions of the General Data Protection Regulation 2018 may be addressed to the Information Standards Officer, and if unresolved, to the Information Commissioner's Office – contact details of both are as follows:

Martina Dalton
Information Standards Officer
NI Assembly, Parliament Buildings, Ballymiscaw, Stormont, Belfast, BT4 3XX
Tel: (028) 90521147 (Ext 21147)
Email: martina.dalton@niassembly.gov.uk)

Information Commissioner's Office (ICO)
Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

Tel: 0303 123 1113 (or 01625 545745 if you would prefer not to call an '03' number, or +44 1625 545745 if calling from overseas)
Fax: 01625 524510

Further information can be found on the ICO website at: - www.ico.gov.uk

4.2 CCTV Privacy Notice

A CCTV Privacy Notice is available explaining the purpose of the CCTV System, the type of data it records and the NI Assembly's disclosure policy

A copy of CCTV Privacy Notice is published on the Northern Ireland Assembly's Internal and external websites and available on the request.

4.3 System Manager

The CCTV System Manager (Head of Usher Services) has day-to-day responsibility for the overall management and operation of the CCTV System, and for ensuring that the policy is fully complied with. Line management and supervisors will directly support the Head of Usher Services in this regard.

4.4 System Operators

The CCTV System Operators working within the Assembly Control Room are required to fully comply with the Operational Procedures Manual and all aspects of CCTV policy.

4.5 Audit

The operation of CCTV System may be subject to audit at any time by the Assembly Internal Audit Team, or other audit as determined by the Information Commissioner This can include an audit of accuracy of images, data retention and downloading.

Proactive checks by Usher Services line management and supervisors will also take place on a regular basis to ensure full compliance with both CCTV policy and the Operational Procedures Manual.

4.6 Public Information

Policy
A copy of the CCTV policy is accessible on the Assembly website and can also be made available upon request.

Signage
Appropriate CCTV signage will be located at entrances to Parliament Buildings and its environs, and in any internal areas where CCTV cameras are operating.

The size and graphics of the signage complies with RNIB recommendations and will indicate:

- The presence of CCTV monitoring;
- The 'ownership' of the CCTV System;
- Contact telephone number for the CCTV System (028 905 21001).

The Assembly Control Room

5.1 Security Arrangements

Images captured by the CCTV System will be monitored and recorded in the Assembly Control Room, on a 24 hour, 365 day basis.

5.2 Access to the Control room

No unauthorised access to the Assembly Control Room will be permitted. Access will be strictly limited to Control Room Operators on duty, Usher Services management or specified members of Senior Management, PSNI and any other person with statutory powers of entry upon production of appropriate documentation. A list of those members of senior management authorised to access the Assembly Control Room is shown at Appendix (A).

Staff, Members and visitors may be granted access to the Assembly Control Room on a case by case basis, and only then on written authorisation from the Head of Usher Services or the Director of Corporate Services. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Assembly Control Room.

Before allowing access to the Assembly Control Room, Control Room Operators will satisfy themselves of the identity of any visitor, and they will ensure that the visitor has appropriate authorisation.

All visitors will be required to complete and sign the visitors' log, which shall include details of their names, their departments or the organisations they represent, the person who granted authorisation and the times of entry and exit.

A similar log will be kept of the staff on duty in the Assembly Control Room and of any visitors granted emergency access.

5.3 Security Control Administration and Procedures

Details of the administrative procedures which apply to the Assembly Control Room will be set out in the Operational Procedures manual which is available for inspection by prior arrangement.

Images of identifiable living individuals are subject to the provisions of the General Data Protection Regulation 2018. All recordings will be handled in strict accordance with this policy and the procedures set out in the Operational Procedures Manual.

5.4 Staff

All staff working in the Assembly Control Room have been made aware of the sensitivity of handling CCTV images and recordings. Head of Usher Services will ensure that all staff are fully briefed and trained in respect of all functions relative to the use of the CCTV system.

All Assembly Control Room Operators will receive refresher training on an annual basis. Training in the requirements of the General Data Protection Regulation 2018 or other relevant legislation will be given by the Information Standards Officer to all those required to work in the Assembly Control Room.

Maintenance of the CCTV System

6.1 System Maintenance

To ensure compliance with the appropriate Codes of Practice, and that recorded images continue to be of appropriate evidential quality, the CCTV System shall be fully maintained in accordance with the maintenance agreement.

The maintenance agreement makes provision for a “callout” emergency repair service as well as regular/periodic service checks, and preventative maintenance of the equipment.

It is the responsibility of the Head of Building Services to manage the maintenance contract and maintain appropriate records. Head of Building Services should provide Head of Usher Services with a record of quarterly maintenance checks.

Management of Recorded Material

7.1 Recordings

Digital recordings are obtained from the Assembly’s CCTV system operating in ‘real time’ mode. Images are retained for 30 days from the date of recording, and then automatically erased. On occasion, it may be necessary to retain images for a longer period where a law enforcement agency is investigating a crime or where it is necessary for the Assembly’s own purpose. This must be approved by the Head of Usher Services or Director of Corporate Services.

Whilst images are retained, they will be held within a secure environment and are subject to recorded audit checks. Management procedures for image retention are listed at Appendix C.

7.2 Guiding Principles

Access to recorded material and the use of same will be strictly for the purposes defined in this policy.

Recorded material will not be copied, sold or used for commercial purposes, or for the provision of entertainment, or otherwise made available for any use which is incompatible with this policy.

7.3 Release of data

Every request for the release of personal data generated by this CCTV System must be made to the CCTV System Manager (Head of Usher Services), who will ensure the principles contained within Appendix B of this policy are complied with at all times.

It is intended, unless otherwise required by law, to safeguard all individuals’ rights to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in the policy;

- Access to recorded material will only take place in accordance with the standards outlined in Appendix B of this policy;

Members of the PSNI or any other agency having a statutory authority to investigate offences may, subject to compliance with Appendix B, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the Operational Procedural Manual.

If material is to be shown to witnesses including police officers for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix B of this policy and the Operational Procedures Manual.

Requests by individuals for the release of their own personal data held on this CCTV system must be made in writing to the Information Standards Officer. Subject Access Request Forms are obtainable from the Usher Services Office, or alternatively requests can be submitted in writing via email, post or fax.

The Information Standards Officer will then arrange for a copy of the data to be made and given to the applicant. All communications must go through the Information Standards Officer and a response will be provided within one calendar month of receiving the request.

The General Data Protection Regulation gives the Information Standards Officer the right to refuse a request for a copy of the data, particularly where such access could prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

8.1 Digital Still Camera Image Prints

A print is a hard copy of a digital camera image or images which already exist on the digital hard drive storage unit, and such prints fall within the definition of 'data'.

Prints will not be made as a matter of routine, and each time a print is made, it must be justified by the originator, who will be responsible for recording the full circumstances under which the print is taken in accordance with the Operational Procedures Manual.

Prints contain data and will therefore be released only under the terms of Appendix B of the policy, *'Release of data to third parties'*.

If prints are released to the media (in compliance with Appendix B) in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Operational Procedures Manual.

A record will be maintained of all print productions, and the recorded details will include a sequential number, date, time and location of the incident, date and time of

the production of the print, the identity of the person requesting the print (if relevant) and the purpose for which the print was taken.

The records of the video prints taken will be subject to audit, in common with all other records in the CCTV System.

Appendix A. Authorised access to the Assembly Control Room.

Other than Assembly Control Room Operators on duty, the following persons will have authorised access to the Assembly Control Room.

Clerk/Chief Executive of the Assembly
Director of Corporate Services
Head of Usher Services
Assistant Assembly Clerk Usher Services
Principal and Senior Ushers

Appendix B. Authorised access to CCTV recorded data

Release of Data to Third Parties - general policy

All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests should be made in writing to the Information Standards Officer at the following address:

Information Standards Officer
NI Assembly
Parliament Buildings
Ballymiscaw
Stormont
Belfast
BT4 3XX

Email: info@niassembly.gov.uk

Those authorised access to recordings in order to achieve the purposes of the system

Clerk/Chief Executive of the Assembly
Director of Corporate Services
Head of Usher Services
Assistant Assembly Clerk Usher Services
Principal and Senior Ushers

Request to View Data

All requests to view data generated by the CCTV System, should be addressed to the Information Standards Officer and should be processed on the provision that:

- The request is made in writing;
- Sufficient information is supplied to identify the person making the request;
- Sufficient and accurate information about the time, date and location is supplied, to enable the retrieval of the information;
- The reason for the request and the purported lawful basis of the request is supplied;
- The person making the request is shown only information relevant to that particular request and which contains personal data of her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure, or it is reasonable in all the circumstances to disclose the information in the absence of such consent.

Before complying with a request, management will ensure the following:

- The request does not contravene and compliance would not be in breach of current relevant legislation,
- Any legislative requirements have been complied with

If in compliance with a request to view data, a decision is taken to release material to a third party including PSNI, written agreement to release the material will be sought from the Head of Usher Services and the Information Standards Officer.

In complying with a request to supply a copy of the data to the data subject, only data pertaining to the individual should be copied and provided. All other personal data which might facilitate the identification of any other person should be concealed or erased.

In addition to the principles contained within the General Data Protection Regulation the NIA will ensure the data is:

- Not the subject of a complaint or dispute which has not been actioned;
- Original data and that the audit trail has been maintained;
- Not removed nor copied without proper authority;
- For individual disclosure only (i.e. to be disclosed to a named subject)

<u>Process of Disclosure</u>

Before complying with a request, management will ensure the following:

- The accuracy of the request is verified.

- The data is replayed to the requester only (or person lawfully acting on behalf of the person making the request).

- The viewing takes place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.

- It must not be possible to identify any other individual from the information being shown (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).

- If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be redacted prior to being sent to the person requesting the data.

Media disclosure

In the event of a request from the media for access to recorded material, the procedures outlined below shall be followed:

- The release of the material must be accompanied by a signed release document that clearly states what the data will be used for, sets out the limits on its use, and indemnifies the partnership against any breaches of the legislation.

- The release form shall state that the receiver must process the data in a manner prescribed by the Assembly Commission e.g. specific identities/data that must not be revealed.

- It shall require that proof of any editing must be passed back to the NIA, either for approval or final consent, prior to its intended use by the media (thus protecting the position of the Assembly Commission who would be responsible for any infringement of the General Data Protection Regulation and the CCTV System's Code of Practice).

- The release form shall be considered a contract and signed by both parties.

Appendix C. NI Assembly CCTV Image Retention Policy

1. Aim

1.1. The aim of this policy is to ensure compliance with the General Data Protection Regulation, Human Rights Act and any best practice as laid down by the Information Commissioners Office.

2. Overview

2.1. The General Data Protection Regulation does not prescribe any specific minimum or maximum retention periods that apply to CCTV systems.

2.2. Retention should not be for any purpose incompatible with the Assembly's own purpose for recording images.

2.3. Images should not be kept for longer than necessary. On occasion it may be necessary to retain images for a longer period where a law enforcement body is investigating a crime to give them opportunity to view the images as part of an active investigation.

2.4. Regular systematic checks of retained images are to be conducted to ensure best practice and policy compliance.

3. Assembly CCTV Image Storage and Access

3.1. Images recorded on the Assembly's CCTV system are held for 30 days and are then automatically erased.

3.2. Where images are retained, they are kept within a secure environment and access to the images is restricted to authorised personnel only.

4. Image Retention Guidelines

4.1. Retained images will be fully documented.

4.2. Images must not be retained for longer than is necessary for a particular specified and lawful purpose.

4.3. Once a retention period has expired, the images must be securely erased and that erasure documented.

4.4. If images are kept for evidential purpose, they are to be kept in a secure place in accordance with Information Assurance Policy (http://assist.assemblyni.gov.uk/services/information_off/recmgt/documents/info_assurance_policy.pdf) with controlled documented access.

4.5. Digital images will be securely retained within the *Synectics Review Client Locker*, unless the Data Controller authorises a copy (DVD) to be made.

5. Documenting the Retention of CCTV Images

5.1. The following details are to be recorded when images are retained.

- The date/time at which the images were retained.
- Name of person retaining the images.
- Review date for the end of the retention period.

- The reason for retaining the images.
- Any PSNI crime number to which the images are relevant.

6. Documenting the Destruction of Images

6.1. The destruction of CCTV images is to be undertaken by an authorised person and countersigned by a line manager.

6.2. The following details below are to be recorded when images are deleted.

- Name and signature of person deleting the images.
- Date/time of deletion of images.
- Reason for deletion of images.
- Name and signature of person witnessing deletion of images.

Note: Images refers to digital data that is held within the '*Synectics Review Client Locker*', or a copy held on DVD.

7. Regular Systematic Checks of the Retention Process

7.1. Audits of images that have been retained are to be conducted by Usher Services management to ensure that the Retention procedure is being complied with and that results are recorded, as explained below.

- Name of person conducting Retention procedure checks.
- Date/time of Retention procedure checks.
- Number of images being retained.
- Reason for retention of each image.
- Compliance of retention period for each image
- Security of images being retained (Access to retained images restricted to authorised personnel only)

8. List of Authorised Persons

8.1. The following persons are authorised to have access to images held within the Assembly Security Management System:

- Head of Usher Services
- Data Controller
- Principal and Senior Ushers
- Authorised Contractors (when conducting repairs/maintenance only)

- Persons who have received written authorisation of access from the Head of Usher Services.

9. Authorised Persons Duties

9.1. Authorised persons have the authority to perform the following duties in relation to the retention of images:

- Retain images on the *Synectics Review Client locker*. (Subject to the Image Retention Guidelines)
- Copy images onto DVD when authorised by the Data Controller and in accordance with the policy.
- Review and delete images that are no longer required, to ensure best practice and compliance with the legislation and Image Retention Guidelines
- Maintain and update the relevant documentation.
- Conduct systematic checks of the retention process to ensure compliance.
- Give authority for repairs / maintenance to the image retention systems.

Appendix D. Parliament Buildings' Areas Covered by CCTV

- East and West barriers and entrance routes
- Upper East and West Car Parks
- The building frontage including steps and apron
- All building access points
- Basement corridors leading from access points
- The Great Hall
- All first floor galleries in the Commons Chamber