# CCTV Policy and Procedures

<table>
<thead>
<tr>
<th>Policy reference number</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>CCTV Policy and Procedures</td>
</tr>
<tr>
<td>Responsible committee and officer</td>
<td>Head of Finance</td>
</tr>
<tr>
<td>Original author:</td>
<td>Head of Finance</td>
</tr>
<tr>
<td>Current revision author: (if applicable)</td>
<td></td>
</tr>
</tbody>
</table>

## Approval

<table>
<thead>
<tr>
<th>Version</th>
<th>Date approved</th>
<th>Approving committee</th>
<th>Individuals/groups to be notified (if relevant)</th>
<th>Committee officer signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Purpose/change</th>
<th>Review date</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>14/11/19</td>
<td>Head of Finance</td>
<td>Approved by Principal</td>
<td>Nov 20</td>
</tr>
</tbody>
</table>
Contents

1  Introduction............................................................................................................. 4
2  Data Protection Legislation ..................................................................................... 4
3  Purpose of the System ........................................................................................... 4
4  The System ............................................................................................................ 5
5  Access to the System ............................................................................................. 5
6  Recording and Storage ........................................................................................... 5
7  Covert recording ..................................................................................................... 6
8  Signage .................................................................................................................. 6
9  Staff Training .......................................................................................................... 6
10 Disclosure............................................................................................................... 7
11 Access to Images – by a Subject ............................................................................ 7
12 Privacy Notice ........................................................................................................ 8
13 Complaints ............................................................................................................. 8
1 Introduction

1.1 Lews Castle College has in place a CCTV surveillance system. Images are monitored and recorded centrally and will be used in strict accordance with this policy. The system is owned by Lews Castle College UHI, Stornoway, Isle of Lewis, HS2 0XR.

1.2 The Head of Finance is responsible for the operation of the system and for ensuring compliance with this policy.

2 Data Protection Legislation

2.1 CCTV digital images, if they show an identifiable person, are personal data and are covered by Data Protection legislation. This Policy should be read in association with Lews Castle College UHI Data Protection Policy, the provisions of which should be adhered to at all times.

3 Purpose of the System

3.1 The system has been installed by Lews Castle College UHI with the primary purpose of reducing the threat of crime generally, protecting the security of and preventing damage to Lews Castle College UHI premises, helping to ensure the health, safety and wellbeing of all Lews Castle College UHI staff, students and visitors and providing evidence for insurance claims or legal proceedings whilst maintaining respect for individuals’ rights to privacy.

3.2 These purposes will be achieved by monitoring the system to:

- deter individuals who have criminal intent;
- assist in the detection of crime;
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order;
- facilitate the identification of any activities / event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and / or to a member of staff or student against whom disciplinary action is being taken or investigated;
- provide evidence of incidents that may lead to insurance claims or legal proceedings;
- facilitate the movement of vehicles on site.

3.3 The system will not be used:

- to provide recorded images for any purpose other than specified under this policy or required for a legitimate legal purpose;
- to record sound;
- for any automated decision-taking.
4 The System

4.1 The system comprises: fixed position cameras; pan tilt and zoom cameras; monitors; multiplexers; digital recorders; public information signs.

4.2 Cameras are located at strategic points, principally but not exclusively at the entrance and exit points of buildings. No camera will be hidden from view. Cameras will be prevented from focusing on the frontages or rear areas of private accommodation.

4.3 Images captured by the system will be recorded twenty-four hours a day throughout the whole year.

4.4 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

5 Access to the System

5.1 Monitors are not visible from outside the room where the equipment is located. The monitor is kept in a locked cabinet to prevent unauthorised access to live images.

5.2 No unauthorised access to the CCTV equipment will be permitted at any time. Access will be strictly limited to Estates staff, the Head of Finance, the Principal, police officers, and any other person with statutory powers of access and any person who requires access for the purpose of maintenance of the system.

5.3 Any other staff, students or visitors may only be granted access to the CCTV system on the written authorisation of the Head of Finance or the Principal.

5.4 Before allowing access to the equipment, staff will satisfy themselves of the identity of the person and that they have appropriate authorisation. The details of any external person given access to the system will be required to complete and sign the access log, including details of their name, department or organisation, the nature of their authorisation, and the time of access to the system.

6 Recording and Storage

6.1 Digital recordings are made using digital video recorders in real time.

6.2 Images will normally be retained for thirty days from the date of recording and then automatically over-written and the log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the log will be updated accordingly.

6.3 All hard drives and records shall remain the property of Lews Castle College UHI until disposal and destruction.
7 Covert recording

7.1 Covert cameras are not currently in use, but may be used under the following circumstances on the written authorisation of the Principal where it has been assessed by the Head of Finance that:

- informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place

7.2 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

7.3 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached, and the Data Protection Officer will be advised.

7.4 Any covert recordings on mobile equipment will be encrypted to ensure data is protected in accordance with the regulations.

7.5 Covert recordings will be restricted to cover only public areas that are not covered by the fixed CCTV installation.

8 Signage

8.1 Clearly visible signs are put up to ensure that anyone likely to be captured by the cameras is aware of them.

8.2 Information is available on the College website (through the web publication of this Policy and Procedures document) about the system, including how individuals may exercise their rights and how long images are stored.

8.3 Information is included in the campus information leaflet provided to visitors, staff and students in the Stornoway Campus.

9 Staff Training

9.1 All staff with access to the system are made aware of the sensitivity of handling CCTV images and recordings.

9.2 Training in the requirements of Data Protection legislation and on the relevant College policies and procedures is given to all those with access to the system.
10 Disclosure

10.1 Disclosure of recorded material will only be made to third parties in strict accordance with the stated purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder including the media where the assistance of the general public is required in the identification of a victim of crime or in the identification of a perpetrator of a crime;
- Prosecution agencies;
- Relevant legal representatives;
- Insurance representatives (in the event of a claim);
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings;
- Emergency services in connection with the investigation of an accident or incident.

10.2 Where disclosure is required, information will be redacted to protect the identity of any people unconnected with the purpose for which the data is being provided.

11 Access to Images – by a Subject

11.1 CCTV digital images, if they show a recognisable person, are personal data and are covered by Data Protection legislation. Anyone who believes that they have been recorded on CCTV is entitled to ask for a copy of the data, subject to exemptions contained in Data Protection legislation. There is no entitlement to instant access.

11.2 A person whose image has been recorded and retained and who wishes access to the data must make a Subject Access Request in writing to the local data protection contact at: lefoi@uhi.ac.uk

11.3 The request must clearly specify what information is being requested, including the date and approximate time the images were captured in order for the data to be located and retrieved.

11.4 The Data Protection Officer will then arrange for a copy of the data to be made and, if appropriate, given to the person. The person must not ask another member of staff to show them the data, or ask anyone else for a copy of the data.

11.5 A response will be provided promptly and in any event within one calendar month of receiving the Subject Access Request.

11.6 Data Protection legislation gives the Data Protection Officer the right to refuse a request for a copy of the data where exemptions apply. The Data Protection officer may also redact information in order to protect the identity of other individuals or to ensure other confidential or exempt information is not provided.
11.7 If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject will be informed in writing of the decision.

**12 Privacy Notice**

12.1 Individuals have rights under Data Protection legislation in relation to the way their information is processed. This is detailed in the relevant Privacy Notice.

**13 Complaints**

13.1 If an individual is unhappy about the way their data has been processed, they may make a complaint to the Information Commissioner’s Office. The Information Commissioner’s Office is UK’s independent authority set up to uphold information rights in the public interest. Their website is [www.ico.org.uk](http://www.ico.org.uk)