CCTV Policy

Lealands High School

CCTV Policy

Lealands High School

Issue Date: January 2025

1. PURPOSE

1.1 Lealands High School uses CCTV to protect against crime and to protect pupils, staff, parents and members of the public when they are on school premises.

1.2 Images of people captured on CCTV where they can be easily identified are defined as personal data under the Data Protection Act 2018. Lealands High School follows requirements of the Act when using CCTV.

1.3 Lealands High School will comply with this CCTV policy to ensure that the school can justify the use of CCTV under the Data Protection Act 2018 and subsequent guidance released by the Information Commissioner's Office and under the Human Rights Act 1998.

1.4 The policy applies where open use of CCTV is intended in public areas. It does not apply to targeted or covert surveillance activities. Any operation of this kind may only be carried out with reference to the Regulation of Investigatory Powers Act (RIPA) 2000 in consultation with Luton Borough Council Policy and/or the Police.

1.5 This policy applies to all CCTV systems in operation at the school

1.6 This policy will be reviewed as appropriate or as legal advice changes

2. RESPONSIBILITIES FOR CCTV OPERATION

2.1 CCTV schemes will be administered and managed by the Headteacher in accordance with this policy and with guidance from the LA where necessary.

2.2 The day-to-day management of the CCTV scheme will be the responsibility of designated senior leaders and the school's Facilities Management Contractor MITIE. MITIE as the operating authority for CCTV in the school have their own policy detailing operation in school.

2.3 Precautions must be in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to the Data Protection Act 2018 and any security precautions.

2.4 Annual notification for CCTV use is required by the Information Commissioner's Office, checks will be carried out on a regular basis to ensure that all procedures are correctly followed.

3. LEGAL BASIS FOR USE OF CCTV SYSTEMS

3.1 The use of CCTV and the images recorded must comply with the Data Protection principles and must be:

- fairly and lawfully obtained;
- adequate, relevant and not excessive;
- accurate;
- used only for purposes about which people have been informed;
- secure and protected from unauthorised access;
- not held longer than required for the purposes they were recorded;
- accessible only to data subjects where a request has been made under the Data Protection Act and where the images are defined as personal data and do not compromise the safety, security or privacy of other individuals

3.2 In order to use CCTV, Lealands High School must have a legitimate basis for recording the personal data. The legitimate purposes for the basis of CCTV use at Lealands High School are:

- prevention and detection of crime, e.g., theft, arson and criminal damage;
- to protect the school buildings and assets;
- to increase the perception of safety and reduce the fear of crime;
- to protect members of the public and private property;
- to ensure the safety of pupils and others present on school premises.

3.3 The use of CCTV must be fair and must not be excessive or prejudicial to any individual or any group of individuals. In order for the use of CCTV to be fair, Lealands High School has informed people that CCTV is in use on the premises by means of notices at various locations through-out the school

3.4 The Human Rights Act (HRA) gives every individual a right to private life and correspondence. This means that CCTV should not be used inappropriately and in areas where people could expect privacy. The HRA also makes it imperative that people are informed when CCTV is in operation. Therefore, the school does not use CCTV in toilets, changing rooms, offices or individual classrooms.

3.5 Lealands High School has documented the purposes for which CCTV is to be used on the premises through this policy.

4. ENSURING THAT USE OF CCTV IS FAIR

4.1 Lealands High School includes the use of CCTV on their annual Data Protection notification (registration) to the Information Commissioner's Office as one of the purposes for which they use personal data.

4.2 Lealands High School will only use CCTV for the purposes stated. CCTV or images produced from it should not be used for any other purposes, particularly purposes which could not reasonably be envisaged by individuals.

4.3 Lealands High School will ensure that pupils, staff and other people who use their buildings are informed of the use and purpose of CCTV. This has been done by means of clear and obvious notices placed around the school premises. Notices include the following information:

- the identity of the Data Controller (the school);
- the purposes for which CCTV is being used, e.g., for the prevention or detection of crime or to increase safety and security whilst on school premises;
- details of who to contact about the scheme and phone number where applicable.

4.4 The wording of notices at Lealands High School are:

- For your safety and security and for the prevention of crime, closed circuit television operates in this area.

  Operator: Lealands High School Contact: 01582 611600

4.5 CCTV cameras must only record images on school premises and should not be directed at surrounding private property.

4.6 The viewing of CCTV footage will be the responsibility of the Headteacher and a limited number of nominated staff – the Seniore Leadership Team and designated Safeguarding leads . Lealands High School does not permit any third party to view CCTV footage. Images will only be released to a third party where the school is legally obliged to do so and following the guidance set out in the Information Commissioner's Office CCTV Code of Practice (2008), Data Protection Act 2018 and the Human Rights Act 1998.

5. SELECTION, OPERATION AND MAINTENANCE OF CCTV SYSTEMS

5.1 Selecting a system

The CCTV system chosen must be of sufficient quality to ensure that recordings and images produced are useable by the school and the police. When choosing or updating a system, the latest police guidance (which can be found on the Home Office website) should be used. MITIE is responsible for selecting maintaining and upgrading CCTV in accordance with the following principles and under the direction of the Headteacher. In general:

- Digital systems are recommended by the police as they provide good quality recordings and the capacity to produce clips and stills and to copy records to removable media.
- Equipment must work effectively together. For example, a high quality digital CCTV system can only be used to its full capacity if the cameras are also of a similar quality.
- Equipment must be maintained correctly, checked regularly and repaired immediately if faulty, otherwise there is a risk that footage cannot be used in the investigation of a crime.

- Where removable media such as DVD or tape is used, it should be of a high quality and replaced on a regular basis. Each item should be identified by a unique mark and stored in date order where appropriate. Media should be wiped completely before it is re-used.
- Cameras should be sited so that individuals can be recognised easily, where required. Care should be taken that the view from a camera does not become obscured or is positioned to view spaces that is not of relevance to the purposes of your CCTV system.
- The CCTV system used at Lealands High School is Samsung Security Manager.

5.2 **Security**

5.2.1 CCTV equipment should be held in a separate, locked room where possible (or in a locked cupboard where this is not possible) and access must be strictly confined to authorised staff. The systems are password protected to ensure security.

If any emergency or routine maintenance is required on the CCTV system the Facilities Management contractor MITIE must be satisfied of the identity of contractors before allowing access to the equipment.

5.2.2 Remote access to cameras via 'off air' access or via broadband links should be used sparingly. When accessing cameras from home over the Internet, staff should ensure that unauthorised persons cannot view the footage, or safeguards are installed to protect CCTV images from being intercepted.

5.3 **Retention of recordings**

5.3.1 Digital recordings or removable media (i.e. USB's/CD's etc.) must be stored in a separate, locked room (or locked cupboard) and access must be strictly confined to authorised staff. A recording system i.e. dates/times and recording details should also be retained whilst the material is held.

5.3.2 Recordings should be held for a limited length of time and must be destroyed when their use is no longer required. Lealands High School will hold recordings for a maximum period of 28 days; however, this may be extended where the recordings are required for an on-going investigation. When the retention period has been reached, digital recordings or removable media should be destroyed or wiped securely.

6. COVERT SURVEILLANCE

6.1 On the rare occasions when schools may wish to use CCTV covertly (i.e., without making people aware of it), an application must be made under the Regulation of Investigatory Powers Act (RIPA). The school should discuss the matter with Luton Borough Council in order to gain authorisation.

6.2 Where the police wish to undertake convert surveillance, they will obtain the relevant authorisation.

7. PROCEDURES FOR DISCLOSURE OF CCTV RECORDS TO OTHER ORGANISATIONS

7.1 Access to CCTV recordings day-to-day is restricted to nominated senior staff who operate the system.

7.2 CCTV recordings are held only by the school unless there is a legal obligation to disclose them. Disclosure includes the viewing of images by someone who is not the operator of the system as well as the transfer of recordings to another organisation. Lealands High School does not permit any third party to view CCTV footage. Images will only be released to a third party where the school is legally obliged to do so and following the guidance set out in the Information Commissioner's Office CCTV Code of Practice (2008), Data Protection Act 2018 and the Human Rights Act 1998.

7.3 Records may need to be disclosed for the following reasons:

- to the police, for the prevention and detection of crime;
- to a court for legal proceedings;
- to a solicitor for legal proceedings;
- to the media for the purposes of identification.

7.4 Where recordings have been disclosed or viewed by an authorised third party the school must keep a record of:

- when the images were disclosed;
- why they have been disclosed;
- any crime incident number to which they refer;
- who the images have been viewed by or disclosed to.

7.5 Viewing of CCTV recordings by the police must be recorded in writing. Requests by the police are actioned under section 29 of the Data Protection Act. The police should provide a completed section 29 form stating that the information is required for the prevention and detection of crime. If a form is not available, or in an emergency, the school must record in writing when and why the information has been released.

7.6 Should a recording be required as evidence, a copy may be released to the police. Where this occurs the recording will remain the property of the school. The date of the release and the purpose for which it is to be used must be recorded.

7.7 The police may require the school to retain recordings for possible use as evidence in the future. Such records must be stored and indexed so that they can be retrieved when required.

7.8 Applications received from other outside bodies (e.g solicitors) to view or release recordings will be referred to the Headteacher. In these circumstances, recordings are only likely to be released for legal proceedings, following an information access request (see section 8) or in response to a Court Order.

7.9 Recordings will only be released to the media for use in the investigation of a specific crime and with the written agreement of the police.

8. SUBJECT ACCESS REQUESTS

8.1 Under section 7 of the Data Protection Act 2018, individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Act. If a request is received, a fee (up to a maximum £10) can be charged and a copy of the images must be provided within 1 calendar month of the request.

8.2 Recent legal cases have raised the issue of when CCTV images should be considered as personal data. Guidance arising from this implies that personal data must be substantially about the person and should affect their privacy in some way. In relation to CCTV this will not include all images:

- A wide shot of, for example, a playground or school corridor with many people in view of the cameras would not normally be considered as the personal data of all those involved. However, where a camera has picked up an individual or group of individuals specifically, or has been moved to zoom in on them, the images recorded can be considered personal data.

8.3 Where a request has been made to view an image or recording, an application must be made in writing, together with details of themselves to allow the school to identify them as the subject of the images and to locate the images on the system. The individual may wish to access either a still image or part of a recording. Where third parties are included in the images, they should be removed where this is technically possible. Where removal is not possible, a balanced decision needs to be made, which considers whether the images would involve an unfair intrusion into the privacy of third parties in the image(s), cause unwarranted harm or distress, and whether it is reasonable in all circumstances to release the information to the individual.

8.4 There is no obligation to provide information where a request has been made after CCTV records have been routinely destroyed in accordance with this policy - see 5.5 (i.e. for recordings that no longer exist). However, where a request has been made for recordings still in existence, they must not be destroyed until the request is complete.

8.5 The school will liaise with the Local Authority's Data Protection Officer.

9. BREACHES OF POLICY

9.1 Any breach or alleged breach of this policy or school guidelines on the use of CCTV by school staff or other individuals will be investigated by the Headteacher.

9.2 An investigation will be carried out into any breaches of policy and procedures reviewed or put in place to ensure that the situation does not arise again.

10. COMPLAINTS

10.1 Any complaints about the operation of the CCTV system should be addressed to the Headteacher, where they will be dealt with according to the school's standard complaints procedures, with reference to this policy.

11. REFERENCES AND LINKS

Information Commissioners Office: ICO - CCTV

CCTV Code of Practice (revised edition 2008): Code of Practice

To view the schools data registration with the Information Commissioner's Office please enter the schools registration reference number, Z6283228, into the search option of the following link to the Information Commissioner's Officers data register:

https://ico.org.uk/what_we_cover/register_of_data_controllers

APPENDIX A

Checklist for users of limited CCTV systems monitoring small retails and business premises (taken from the document – In the picture: A data protection code of practice for surveillance cameras and personal information published by the Information Commissioners Office).

The CCTV system and the images produced by it are controlled by the Headteacher of Lealands High School who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 2018).

Lealands High School has considered the need for using CCTV and have decided that it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	CHECKED (date)	**BY**	**DATE OF NEXT REVIEW**
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	10/01/2025 Renewal was submitted to the ICO in January 2022 2021. Next renewal date 17/01/2025.	Johanna Goslin	10/01/2028
There is a named individual who is responsible for the operation of the system.	10/01/2025 The Headteacher is responsible for the operation of the system with delegated powers given to some senior staff and MITIE the facilities management contractor.	Johanna Goslin	10/01/2028
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.	10/01/2025 Cameras have been installed for the following purposes: • Prevention and detection of crime • Protect the school buildings and assets • Increase the perception of safety and reduce fear of crime • Protect members of the public and private property • Ensure the safety of pupils and others present on school premises • CCTV is the best solution to support addressing the identified problems.	Johanna Goslin	10/01/2028
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	10/01/2025 iVMS Manager is the CCTV system installed at the school. It produces clear images which can be taken from the system when required.	Johanna Goslin	10/01/2028
Cameras have been sited so that they provide clear images.	10/01/2025 Cameras have been positioned throughout the premises to provide clear images which are not obscured by buildings or	Johanna Goslin	10/01/2028

	CHECKED (date)	BY	DATE OF NEXT REVIEW
	equipment etc.		
Cameras have been positioned to avoid capturing the images of persons not visiting the premises	10/01/2025 Cameras have been positions to capture images of the school buildings and grounds only.	Johanna Goslin	10/01/2028
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	10/01/2025 There are a number of signs located on entrances to the school.	Johanna Goslin	10/01/2028
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	10/01/2025 The CCTV system is only accessible from secure offices and the system is password protected. If any images are taken from the system these are always securely stored.	Johanna Goslin	10/01/2028
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	10/01/2025 Recorded images are kept for a maximum of 28 days unless this is required for an on-going investigation.	Johanna Goslin	10/01/2028
Except for law enforcement bodies, images will not be provided to third parties.	10/01/2025 Images are not provided to third parties unless there is a legal obligation to provide them.	Johanna Goslin	10/01/2028
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	10/01/2025 The impact on individuals' privacy has been identified and taken into account.	Johanna Goslin	10/01/2028
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such as request is made.	10/01/2025 Subject access requests are detailed in the schools CCTV policy.	Johanna Goslin	10/01/2028
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	10/01/2025 Weekly checks are completed by MITIE on the CCTV system to ensure that the system is working properly.	Johanna Goslin	10/01/2028