



Lake Haven CCTV Policy

Date approved by Alexandra Marshall	August 2022
Renewed	July 2025
Renewal Date*:	July 2028

This policy will be reviewed and updated as necessary if/when any changes are made to legislation that affect our practice. Otherwise, or from then on, this policy will be reviewed every 3 years and shared with all staff at Lake Haven.

1. Introduction

Lake Haven uses Close Circuit Television (CCTV) within the premises of our school. Ensuring that Lake Haven premises are safe, protected places where children can thrive in their education is the non-negotiable starting point for each school day. CCTV is just one measure in place to support the children and staff to feel secure and happy at the school.

This policy sets out clear expectations of the school with regard to the management, operation and use of CCTV within Lake Haven.

2. What is the purpose of this policy?

2.1 The purpose of this policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Lake Haven.

2.2 This policy applies to all members of our workforce, visitors to school and Central Team premises and all other persons whose images may be captured by the CCTV system.

2.3 This policy takes account of all applicable legislation and guidance, including:

2.3.1 General Data Protection Regulation ("GDPR")

2.3.2 [Data Protection Act 2018] (together the Data Protection Legislation)

2.3.3 CCTV Code of Practice produced by the Information Commissioner

2.3.4 Human Rights Act 1998

2.4 CCTV cameras are installed externally around the premises for the purposes of enhancing security of the building and its associated equipment.

2.4.1 To provide a safe and secure environment for pupils staff and visitors

2.4.2 To enhance the security of the buildings and its associated equipment, to prevent the loss of or damage to the schools buildings and/or assets

2.4.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

2.5 CCTV surveillance of Trust premises is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and

2.6 The system does sound recording capability.

2.7 The CCTV system is owned and operated by Lake Haven School, the deployment of which is determined by the Headteacher.

2.8 The CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016/679.

2.9 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

3. Links with other school policies and practices

This policy links with several school policies, practices and action plans including:

- o Lake Haven GDPR Policy
- o Lake Haven Policy
- o Lake Haven School Staff Handbook

4. What is the scope of this policy?

4.1 This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The School complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use.

4.2 CCTV signs will be clearly and prominently placed at the main external entrance to the school. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the school will ensure that there are prominent signs placed within the controlled area.

4.3 This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc. Video monitoring of public areas for security purposes within school premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

4.4 All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the school. Recognisable images captured by CCTV

systems are 'personal data'. They are therefore subject to the provisions of the General Data Protection Regulation and Data Protection Act 2018

5. Location of Cameras

5.1 The cameras are sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated. Lake Haven school will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation. (A map of CCTV cameras on site will be maintained by the Headteacher)

5.2 Lake Haven will make every effort to position the cameras so that their coverage is restricted to the school premises, which includes outdoor areas. CCTV is limited to the external perimeters and access points to the school and will not be used in classrooms or internal areas of the school. Members of staff will have access to details of where CCTV cameras are situated

5.3 CCTV Video Monitoring and Recording of Public Areas may include the following:

5.3.1.1 Protection of school buildings and property: The building's perimeter, entrances and exits

5.3.1.2 Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms

5.3.1.3 Video Patrol of Public Areas: Parking areas, Main entrance/exit gates

5.3.1.4 Criminal Investigations (carried out by the police): Robbery, burglary and theft surveillance

6. Who is responsible?

6.1 Access to the CCTV is password protected and only those named in this policy have permission to access the CCTV images and recordings as part of the school's monitoring systems and processes as set out in this policy.

6.2 *Staff authorised access* is restricted as determined by the school.

6.3 The Headteacher will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy.
- Oversee the use of CCTV monitoring for safety and security purposes within the school.
- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Monitor the school's CCTV Access Log and any release of tapes or any material recorded or stored in the system.
- Authorise and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally, including reviewing camera locations
- Give consideration to members of the school community's feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place.
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that images recorded are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Headteacher.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

- Hold to account any member of staff who uses the CCTV for purposes other than those stated in this policy.

6.4 The School Business Manager will:

- Oversee and coordinate the use of CCTV monitoring for safety and security purposes within the school.
- Maintain the school's CCTV Access Log to record the use of CCTV.
- Document the release of tapes or any material recorded or stored in the system as part of the school's CCTV Access Log.
- Support the Headteacher in the effective implementation of this policy.
- Report concerns, system failures or breaches of this policy immediately to the Headteacher.
- Liaise with the CCTV contractors to make any necessary adjustments to cameras or monitoring checks to ensure compliance with this policy.
- check the CCTV on a weekly basis to ensure that it is operating effectively.

6.5 The Proprietary Body will:

- Ensure the Headteacher and Senior Leads named above, abide by this policy.
- Ensure the school is compliance with this policy.
- Monitor and review this policy.

7 Storage and Retention of CCTV Images

7.1 Recorded data will not be retained for longer than 31 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

7.2 The Data Protection Act and GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Therefore, retention will reflect the school's purposes for recording information, and how long it is needed to achieve this purpose.

7.3 Lake Haven will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The school will store data securely at all times. Data is stored on the CCTV DVR. The measures in place include:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to make copies to specified members of staff

7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the school.

8. Access to CCTV Images

8.1 Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher.

8.2 The Headteacher may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

9. Disclosure of Images / Subject Access Request (SAR)

9.1 Subject Access Requests will be handled in accordance with the Lake Haven GDPR Policy and Subject Access Request Policies.

9.2 All requests should be made in writing to the Data Protection Officer who can be contacted by email at a.marshall@lakehavenschool.co.uk Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: time, date and location.

9.3 Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act and the GDPR.

9.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Headteacher must take appropriate measures to ensure that the footage is restricted in this way.

9.5 If the footage contains images of other individuals then the school must consider

whether:

9.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

9.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

9.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

9.6 A record must be kept, and held securely, of all disclosures which sets out:

9.6.1 When the request was made;

9.6.2 The process followed by Headteacher in determining whether the images contained third parties;

9.6.3 The considerations as to whether to allow access to those images;

9.6.4 The individuals that were permitted to view the images and when; and

9.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

9.7 In the event that the school does not have a facility to provide copies of CCTV footage, the applicant may instead view the CCTV footage if available.

9.8 The school reserves the right to refuse access to CCTV footage where this would; prejudice the legal rights of other individuals, jeopardise an on-going investigation or put at risk the safeguarding of a child.

10. Access and Disclosure of Images to Third Parties

10.1 The school will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

10.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

10.3 If a request is received from a law enforcement agency for disclosure of CCTV images then the Headteacher must follow the same process as above in relation to subject access requests. Details should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

10.4 The information above must be recorded in relation to any disclosure.

10.5 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

11. Privacy Impact Assessment

11.1 Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the school to ensure that the proposed installation is compliant with legislation and ICO guidance.

11.2 The school will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

12. Misuse of CCTV System

12.1 The misuse of the CCTV system could constitute a criminal offence.

12.2 Any member of staff who breaches this policy may be subject to disciplinary action.

13. Complaints relating to this policy

Any complaints relating to this policy or to the CCTV system operated by the school should be made in accordance with the Lake Haven Complaints Policy.

14. Review of this policy

14.1 This policy will be reviewed every three years unless required sooner.

14.2 The CCTV system and the privacy impact assessment (Appendix 1) relating to it will be reviewed every three years.

CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE

1 Who will be captured on CCTV?

[Pupils, staff, parents / carers, volunteers, proprietors and other visitors including members of the public etc]

2 What personal data will be processed?

Facial Images, behaviour

3 What are the purposes for operating the CCTV system?

Prevention or detection of crime due to locality and history of issues on site

4 What is the lawful basis for operating the CCTV system?

[Legal Obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime]

5 Who is/are the named person(s) responsible for the operation of the system?

Lindsay Taylor and Alexandra Marshall

6 Describe the CCTV system, including:

- a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;
- b. siting of the cameras and why such locations were chosen;
- c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

e. whether the system enables third party data to be redacted, for example via blurring of details of third-party individuals.

7 Set out the details of any sharing with third parties, including processors

[Police, subject access, etc. Careful consideration should be given to whether any provider is used in relation to the CCTV system and the access they might have to images. Will those processors send this data outside of the EEA, for example for storage in a cloud-based system?]

8 Set out the retention period of any recordings, including why those periods have been chosen

e.g. All recordings are kept for 30 days, after which time they are automatically destroyed. Recordings of incidents that require investigating will be kept for up to one year. In the event that a recording is required for a longer period, individuals will be notified.

e.g. Recordings passed on to third parties would be kept in accordance with the third parties' retention periods.

9 Set out the security measures in place to ensure that recordings are captured and stored securely

[The CCTV images are held on a password protected system with only the named persons authorised to operate the system having access to the recording].

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings? What measures are in place to address the risks identified?

For example:

- Is it fair to record them in the way proposed?
- How is the amount of data processed to be minimised?
- What are the risks of the system being accessed unlawfully?
- What are the potential data breach risks?

- What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?
- The risk of a potential data breach is minimised as authorised persons must be in pairs to view recordings and protocols around the use of the images are robustly monitored.
- The risks during any transfer of recordings, or when disclosed to third parties such as the police are that 3rd parties may not adhere to GDPR regulations. The school minimises this risk by requiring all third parties to sign for transfer of files in accordance with our policy.

11 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

12 When will this privacy impact assessment be reviewed?

Approval:

This assessment was approved by the Data Protection Officer:

DPO

Date

Date of Review Reason for Review Policy Category Further details Staff Who

School CCTV Viewing Log

Has a recording or

Date to destroy

Date of deletion

Policy Reasons for Review

- Protecting the school buildings and school assets, both during and after school hours;
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- Supporting the police in a bid to deter and detect crime;
- Assisting in identifying, apprehending and prosecuting offenders
- Ensure the safety of staff, children and members of the public whilst on site

DELETE BEFORE PUBLISHING

Reviewed CCTV Action Taken Shown to a 3rd Party

Date of 3rd Party Review

Reason shown to a 3rd Party

image been downloaded

Recordings or Images