Leverhulme
Church of England and Community Trust

CCTV Use Policy

Effective from October 2025

Version 3.0

C Davies

Leverhulme Academy Trust Document Control Table			
Document Title :	**CCTV Policy**	**Author name / post:**	**C Davies** **Chief Finance Officer**
Version Number:	**2.0**	**Document Status:**	**Approved**
Date Approved:		**Approved By :**	**Risk and Audit Committee**
Effective Date :	**25th June 2021** **October 2025**	**Date of next review:**	**Summer 2024** **October 2028**
Publication method:	**Every system**	**Date 1st published**	**26/6/21**
Superseded Version:	**Reviewed – No change, other than formatting and logo.**		

Document History		
Version	**Date**	**Notes on Revisions**
1.0	22 May 2019	This is a new policy to be used by all Academies within the Trust. It sets out the required procedures and expectations in using CCTV and how through this policy the Trust ensures full compliance with required legislation.
2.0	25/6/21	Policy reviewed. No change other than updated Trust logo.
3.0	01/10/25	Policy reviewed. 1.0 Change in title from introduction to statement of intent 1.5 Staff access to recorded images updated 2.1 Surveillance code of practice 2022 updated 6.2 Update in relation to access log. 10. New section – Data Protection Impact Assessment 11. New section - Security

1. Statement of intent

1.1 Leverhulme Academy Trust uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for students, staff and visitors, and to prevent the loss or damage to school property.

1.2 The system comprises of cameras both internally and externally to provide coverage of the majority of the site.

1.3 The system does not have sound recording capability except for in the case of the behaviour units whereby it is necessary due the higher likelihood of conflict ensuing in these areas.

1.4 The CCTV system is owned and operated by the school, and its deployment is determined by the school's leadership team.

1.5 Access to other recorded images is restricted to:

- Healthy and Safety Officer
- Office Administrators/Manager
- Site Team
- ICT Support Team
- Senior Leadership Team
- Year Team Staff

1.6 The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act 1998. This policy outlines the school's use of CCTV and how it complies with the Act.

1.7 CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

2.1 The Trust complies with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, and follows the **Information Commissioner's Office (ICO) guidance on CCTV and video surveillance** to ensure that CCTV is used responsibly and in a way that safeguards both trust and confidence in its continued use. The Trust also has regard to the **Surveillance Camera Code of Practice (updated January 2022).**

2.2 CCTV warning signs will be clearly and prominently displayed across the school site.

2.3 The trust has endeavoured to ensure that the CCTV system is both effective and efficient, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3. Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with GDPR.

3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include indoor and outdoor areas.

3.3 CCTV may be used in classrooms where it is deemed there is a high risk of vandalism due to the value of the equipment used in those rooms, such as ICT suites.

3.4 Members of staff should have access to details of where CCTV cameras are situated. The exception stated in the Code of Practice is if cameras are placed for the purpose of covert monitoring (see below).

4. Covert Monitoring

4.1 The school may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances authorisation must be obtained from the Headteacher.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilet cubicles.

5. Storage and Retention of CCTV images

5.1 Recorded data will not be retained for longer than is necessary, (up to a maximum of 7 days) unless part of an ongoing investigation. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely on the network with restricted access by a secure password.

6. Access to CCTV footage

6.1 Access to recorded images will be restricted to those staff authorised to view them (see 1.5).

6.2 Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log, centrally stored at each school.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

7.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The school will respond to requests within one month of receiving the written request. When requests are complex the school has the right to extend this period to two months.

7.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals, jeopardise an ongoing investigation or where there are other parties present in the images.

8. Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

10. Data protection impact assessment (DPIA)

10.1 The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

10.2 The system is used only for the purpose of fulfilling its aims (stated in section 1.)

10.3 When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

10.4 Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

10.5 If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

11. Security

11.1 The ICT manager will be responsible for overseeing the digital security of the CCTV system and footage, the site manager will be responsible for the physical security of the CCTV system and footage

11.2 The system will be checked for faults on a ongoing basis. Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure

11.3.1 Footage will be stored securely and encrypted wherever possible. The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use. Cyber security measures will be put in place to protect the footage from cyber attacks. Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible