CCTV Policy

Aim of the Trust

One community. Many ideas. Everyone's future.

We aim to provide an exceptional education for every child in the Trust through an ethos of collaboration and high aspirations and through the principles of quality learning using curiosity, exploration and discovery.

Links

This policy is linked to:

- Data Protection Policy
- Freedom of Information Policy

Data Protection

Any personal data processed in the delivery of this policy will be processed in accordance with the Data Protection policy.

Personal data is any information relating to an identified or identifiable living individual. An identifying characteristic could include a name, ID number or location data even if it can only be potentially linked to a living individual.

The Langley Academy Trust uses Close Circuit Television ("CCTV") within its premises. The purpose of this policy is to set out the position of the Trust as to the management, operation and use of the CCTV at each of its sites.

This policy applies to all members of staff, visitors to the premises and all other persons whose images may be captured by the CCTV system.

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

- General Data Protection Regulation ("GDPR");
- CCTV Code of Practice produced by the Information Commissioner;
- Human Rights Act 1998.

This policy should be read in conjunction with the Data Protection Policy.

The system comprises a number of internal and external day and night cameras and does not make use of its sound recording capability. The CCTV system is owned and operated by the Trust and the deployment of it is determined by the Executive Principal and Headteachers. The Data Protection Officer ("DPO") or their representative has overall responsibility as delegated by the Data Controller (Board of Directors/Governors).

Access and viewing is restricted and all authorised operators with access to images will be aware of the procedures they are required to follow and their responsibilities under this policy. All employees will be aware of the restrictions in relation to access to, and disclosure of, recorded images. The further

introduction of, or changes to, CCTV monitoring will be subject to consultation with staff where appropriate.

Purpose of CCTV

The Trust uses CCTV for the following purposes:

- to provide a safe and secure environment for pupils, staff and visitors;
- to protect the Trust buildings and assets;
- to assist in reducing the fear of crime and for the protection of private property;
- to assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

Policy Intent

The Trust will:

- notify the Information Commissioners Office of its use of CCTV as part of the annual data protection registration;
- complete a CCTV Privacy Impact Assessment ("PIA") for the use of surveillance CCTV and will update this as appropriate when the system is upgraded or significantly modified;
- treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act/GDPR;
- use cameras to monitor activities within the Trust grounds to identify potential criminal activity for the purpose of securing the safety and well-being of the Trust, as well as for monitoring student behaviour;
- ensure cameras are not directed outside of the Trust site at private property, an individual, their property or a specific group of individuals. The exception to this would be where an authorisation was obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000;
- display CCTV warning signs and these will be clearly and prominently placed at all external entrances of the site where CCTV is in operation, including the gates as this coverage includes trust grounds and the path and driveway leading to the gates.
- the Trust will ensure that there are visible and readable signs placed at both the entrances of the CCTV zones and within the controlled areas and that these will contain details of the purpose for using CCTV.
- not guarantee that the system will or can cover or detect every single incident taking place in the areas of coverage;
- not use data or knowledge for any commercial purpose. Recorded data will only be released for use in the investigation of a specific crime, with the written authority of the Police and in accordance with the Data Protection Act/GDPR.

Siting Cameras

Cameras will be sited so they only capture images relevant to the purposes for which they are installed (as described above) and care will be taken to ensure that reasonable privacy expectations are not violated. For example, cameras will not be placed in areas that are reasonably expected to be private such as in toilets. The Trust will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act/GDPR requirements.

CCTV is not sited in classrooms and will not be used in such, except in exceptional circumstances as detailed below.

Members of staff, on request can access details of CCTV camera locations.

Covert Monitoring

The Trust retains the right in exceptional circumstances to set up covert monitoring. For example:

(i) where there is good cause to suspect that an illegal or serious 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.

In these circumstances, authorisation must be obtained beforehand from the Executive Principal and Headteacher.

Covert Monitoring may take place in classrooms when circumstance (i) and (ii.) are satisfied. Covert Monitoring used in classrooms will never be used to observe or assess a teacher's professional performance, or to contribute to capability proceedings.

Covert Monitoring will cease following completion of the investigation for which it was established

Cameras sited for the purpose of covert monitoring will not be used in areas that are reasonably expected to be private, for example toilets.

Storage and Retention of CCTV images

Recordings are automatically overwritten after 30 days**.** Specific recordings which the Trust wishes to retain will be logged and kept for no longer than is needed to complete the process for which it has been retained. 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. An example of the log can be seen at Appendix A.

All retained data will be stored securely. An electronic file is held on a secure central server where specific CCTV image/recordings are retained. Data retained for a specific purpose is held securely by the administrator. Access by staff to specific recordings is strictly controlled and the process is outlined below.

The Data Protection Act/GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information, which should be informed by the purpose for which the information is collected, and how long it is needed to achieve this purpose. Storage availability is also a factor to be considered in the ability to retain recordings.

Disclosure of Images to Data Subjects (Subject Access Requests)

Any Individual recorded in any CCTV image is a 'data subject' for the purposes of the Data Protection legislation, and has the right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection legislation. Such a request should be considered in the context of the Trust's Freedom of Information Policy.

All requests should be made in writing to the Executive Principle or Data Protection Officer or their representative.

Those who request access must provide you with details that allow you to identify them as the subject of the information and also to locate the information on your system.

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.

When such a request is made the CCTV system administrator (The Site Manager within Facilities) will review the CCTV footage, in accordance with the request.

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 CCTV system administrators must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals then the Trust must consider whether:

- 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 and protect their rights of access to personal data under the Data Protection Act and their rights to privacy under the Human Rights Act;
- their consent could be obtained; and the other individuals in the footage have consented to the disclosure of their images. Individuals who consent have a right to view the images as part of their consent.
- whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request where consent is not obtained.

In line with guidance, Information will be provided promptly and within no longer than 40 calendar days of receiving a request.

The data subject will be provided with a copy of all the information caught by the request that constitutes their personal data, in a permanent form unless:

- the data subject agrees to receive their information in another way, such as by viewing the footage; or
- where the supply of a copy in a permanent form is not possible or would involve disproportionate effort.

Care should be taken to ensure that the method of disclosure is secure to ensure they are only seen by the intended recipient.

The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

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

- when the request was made;
- the process followed by the CCTV system administrators where the images contained third parties;
- the considerations as to whether to allow access to those images;
- the individuals that were permitted to view the images and when; and
- whether a copy of the images was provided, and if so to whom, when and in what format.

Appendix B provides an example of such a record.

Disclosure of Images to Third Parties

Third parties, which are required to show adequate grounds for disclosure of data in accordance with the criteria laid down in legislation. These, may include, but is not limited to:

- police
- statutory authorities with powers to prosecute, (e.g customs and excise, trading standards etc)
- solicitors
- claimants in civil proceedings
- accused persons or defendants in criminal proceedings
- other agencies, according to purpose and legal status, as agreed by the Data Controller and notifed to the information Commissioner

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

Third parties acting on behalf of a 'data subject' will be handled in accordance with the Trust's Freedom of Information Policy.

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

If a request is received from a law enforcement agency for disclosure of CCTV images then the Trust must follow the same process as above in relation to subject access requests. Detail 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.

The information above must be logged in relation to any disclosure (see Appendix B).

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.

Internal Monitoring

The trustees via The Health and Safety Committee should be updated in relation to the number of requests, disclosures and viewing and the Chair notified of any requests from law enforcement agencies.

Access to CCTV Images

The ability to view live and historical CCTV data available via network software is only to be provided at designated locations and to authorised persons only. Direct access to recorded data is limited to the systems administrators, Property Manager, and members of the pastoral team.

Data from CCTV may be used within the Trust's' discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Complaints and enquiries about the operation of CCTV within the Trust should be directed to the Headteacher or Data Protection Officer in the first instance.

Review Date: May 2019
Ratified Date: May 2019
Author: Rhodri Bryant
Date of Next Review: May 2022

Appendix A – Internal Storage Log of stored CCTV images (specific footage stored for longer than standard period)

Date Stored	By whom	Image/file Reference	Reason for retention	State format of image storage (e.g. CD ROM/Hard Drive/Flash drive)	Date footage was erased, by whom and reason	Date Signed off by DPO

Appendix B – External Requests Subject Access & Third Party Request Disclosure Log

NB: Please follow the Freedom of Information Policy procedures before disclosing any data

Date request received and from whom (name & organisation)	Date referred to DPO	Subject Access or Third Party Request	State reason (if third party)	Date & nature of disclosure (viewing or copy of image)	Images viewed/sent (location, date, time of original image/s and internal image reference)	Outcome if applicable