CCTV Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
1	RGR		Trust Board	October 2020	October 2021
2	RGR	Annual review	Trust Board	October 2021	October 2022
3	RGR	Update to UK-GDPR; addition 4.5, 6.8, 10.1, 10.3; Appendix A: masking; 6.1 personnel	Trust Board	October 2022	October 2024

Contents

1 Policy Statement

1.1 Leger Education Trust uses Close Circuit Television ("CCTV") within the premises of its Academies the purpose of this policy is to set out the position of Leger Education Trust as to the management, operation and use of CCTV.

1.2 This policy applies to all members of our Workforce, visitors to any Trust premises and all other persons whose images may be captured by the CCTV system.

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

1.3.1 The UK General Data Protection Regulation ("UK-GDPR").

1.3.2 CCTV Code of Practice produced by the Information Commissioner

1.3.3 Human Rights Act 1998

1.4 This policy has been developed with reference to https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

1.5 This policy sets out the position of the Trust and its Academies in relation to its use of CCTV.

2 Purpose of CCTV

2.1 Leger Education Trust uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for pupils, staff and visitors;

2.1.2 To assist with behaviour management and to ensure pupils take responsibility for their behaviour;

2.1.3 To prevent the loss of or damage to the Trust buildings and/or assets; and

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

3 Description of system

3.1 Cameras are based in internal and external locations within Trust sites, different Trust sites will use analogue or digital cameras that may be fixed or movable.

4 Siting of Cameras

4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Trust will make all reasonable efforts to ensure that areas outside of the Trust premises are not recorded.

4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as toilet cubicles.

4.5 All academies will have information sited at the entrance on who is the data controller for the images and contact details.

5 Privacy Impact Assessment

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

5.2 The Trust 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.

6 Management and Access

6.1 The CCTV system will be managed by Leger Education Trust, the IT Director/Manager and the School Business Manager.

6.2 On a day to day basis the CCTV system will be operated by members of the Academy or Trust site management teams.

6.3 The viewing of live CCTV images will be restricted to Academy and Trust Management & leadership teams.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by Academy and Trust Management & leadership teams. In the case of an incident being recorded on the CCTV images the Trust may share images with limited individuals who it deems are key in the management if the incident.

6.5 In addition, in some circumstances where it is necessary and proportionate to do so, the images may be shown to pupils involved in an incident either for the purpose of allowing that pupil to understand the impact of their behaviour or as part of the disciplinary process.

6.6 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

6.7 The CCTV system is checked on a regular basis by Academy or Trust Site management and IT teams to ensure that it is operating effectively.

6.8 All viewings of CCTV footage will be logged by the member of staff on a central record, including the data, time and location of camera(s).

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored only for a period of 28 days unless there is a specific purpose for which they are retained for a longer period. In such circumstances authorisation for holding recorded images longer than 28 days must be sought form the Principal/Headteacher.

7.3 The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. 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 Trust

8 Disclosure of Images to Data Subjects

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

8.2 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 Subject Access Request Policy.

8.3 When such a request is made a member of the Academy or Trust management or leadership team will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 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 individual member of the Academy or Trust management or leadership team must take appropriate measures to ensure that the footage is restricted in this way.

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

8.5.1 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;

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

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

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

8.6.1 When the request was made;

8.6.2 The process followed by the Academy or Trust Management or Leadership team in determining whether the images contained third parties;

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

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

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

9 Disclosure of Images to Third Parties

9.1 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.

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

9.3 If a request is received from a law enforcement agency for disclosure of CCTV images, then the member of the Academy or Trust Management or leadership 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.

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

9.5 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.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed every 2 years

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed bi-annually.

10.3 CCTV systems will be regularly maintained, in order to prevent the movement of cameras or any other issues with the system.

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

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

12 Complaints relating to this policy

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

Appendix A: Staff CCTV Code of Practice

Introduction and Accountability

Leger Education Trust has comprehensive closed circuit television (CCTV) surveillance systems (the system) across its sites for the purpose of the prevention and detection of crime and the promotion of health, safety and welfare of staff, students and visitors.

The system is owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel.

This staff code of practice has been prepared from the standards set out in the Information Commissioner's Office Code of Practice "In the picture: A data protection code of practice for surveillance cameras and personal information" and the Surveillance Camera Code of Practice 2013 published by the Home Office. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to Trust sites and to ensure that its operation is consistent with the obligations on the Trust as imposed by UK-GDPR.

In line with the Home Office 12-point code of conduct the use of the system will:

- always be for the purpose specified which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
- take into account its effect on individuals and their privacy
- have as much transparency as possible, including a published contact point for access to information and complaints
- have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
- have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
- have no more images and information stored than that which is strictly required
- restrict access to retained images and information with clear rules on who can gain access
- consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
- be subject to appropriate security measures to safeguard against unauthorised access and use
- have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
- be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim
- be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes

The primary purpose of the system is to:

- To protect the Trust buildings and assets
- To increase personal safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the academies through monitoring student behaviour

Operation

The School Business Manager is responsible for the operation of the CCTV system and for ensuring compliance with this code of practice. It is recognised that members of the Trust may have concerns or complaints in respect of the operation of the system and they are required report any breaches. Any concerns in respect of the system's use or regarding compliance with this code of practice should be addressed to the Principal/Headteacher. Breaches of the code of practice by staff monitoring the system could result in disciplinary action and may, in some cases, be a criminal offence.

System
This code of conduct applies to all Trust sites. It will also encompass all other CCTV images that, in due course, are added to the system.

The system is operational and images are capable of being monitored for 24 hours a day throughout the whole year.

Visitors and the general public are made aware of the presence of the system and its ownership by appropriate signage and the publication of this code of practice on the Trust website. The Trust is responsible for the management and processing of images.

To ensure privacy, wherever practicable the cameras are prevented from focusing or dwelling on domestic accommodation. If the trust has any issues with cameras looking at residential buildings, it will look at masking areas of the camera, to ensure the privacy of residents.

Images captured on camera will be recorded on the main CCTV servers which are held in a secure location. Although every effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

For the purposes of the GDPR/DPA (2018), the Data Controller is the Trust and the Trust is legally responsible for the management and maintenance of the CCTV system. No unauthorised access to the system is allowed at any time. Normal access is strictly limited to authorised staff only. Police officers may view recorded material with the consent of the Principal/Headteacher or Director of Operations.

Persons other than those specified may be authorised to access the CCTV material on a case-by-case basis. Written authorisation is required. Each separate visit will require individual authorisation and will be supervised at all times. Such visitors will not be given access to any data which falls within the scope of the Act.

In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to access the CCTV system.
Before granting access to the CCTV system, controllers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors log, which shall include their name, department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the start and finish times of their access to the CCTV system.

It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures. The Director of Operations will be responsible for the development of, and compliance with, the working procedures of the system.

Recorded images will only be reviewed with the authority of the Principal/Headteacher and in their absence the Director of Operations. Copies of digital images will only be made for the purposes of crime detection, evidence in relation to matters affecting safety, evidence for prosecutions, or where otherwise required by law.

All staff involved in the operation of the CCTV system will, by training and access to this code of practice, be made aware of the sensitivity of handling CCTV images and recordings.

The School Business Manager will ensure that all staff, including relief staff, are fully briefed and trained in respect of all functions; operational and administrative, arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this code of practice will also be provided.

Recordings
The system is supported by digital recording facilities which will function throughout operations in real time.

As the images are recorded digitally, the process of identifying retrieval dates and times will be computerised. Images will be cleared automatically after a set time.

Unless required for evidential purposes or the investigation of crime, recorded images will be retained for no longer than 28 days from the date of recording. However, the Trust recognises that, in accordance with the requirements of the Data Protection Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images. Digital images will be automatically erased after a set period, which will be no longer than 28 days.

In the event of the digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

Digital Recording and Access Procedures
All recordings containing images to and remain the property of the Trust. Recordings are saved to the network using IP addresses, or to a local hard drive. Disk handling procedures are in place to ensure the integrity of the image information held.
Requests by persons outside the Trust for viewing or copying of disks or obtaining digital recordings will be assessed on a case by case basis.
Requests from the police will arise in a number of ways, including:

- requests for a review of recordings in order to trace incidents that have been reported
- immediate action relating to live incidents, e.g. immediate pursuit
- for major incidents that occur when images may have been recorded continuously
- individual police officers seeking to review recorded images on screen
- Viewing of the CCTV by police will be subject to the Principal/Headteacher making an assessment, on behalf of the Trust, of the genuine need to see the recording.

Requests for access to recorded images from persons other than the police or the data subject (that is, the person whose image has been captured by the CCTV system) will be considered on a case by case basis. Access to recorded images in these circumstances will only be granted where it is consistent with the obligations placed on the Academy by UK-GDPR.

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the code of practice reflect the Second and Seventh Data Protection Principles of the UK-GDPR.

All staff should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the equipment.

Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances and to the extent required or permitted by law:

- law enforcement agencies where the images recorded would assist in a specific criminal inquiry
- prosecution agencies
- relevant legal representatives
- Health and Safety Executive

- people whose images have been recorded and retained and disclosure is required by virtue of the UK-GDPR.

All requests for access or disclosure will be recorded. The Principal/Headteacher will make decisions on requested access to recorded images by external persons. Requests by the police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a police officer who must indicate that the images are required for the purposes of a specific crime enquiry.

If access or disclosure is denied, the reasons will be documented. If access to or disclosure of the images is allowed then the following will be documented:

- the date and time at which access was allowed or the date on which disclosure was made
- the reason for allowing access or disclosure
- the extent of the information to which access was allowed or which was disclosed

Photographs and hard copy prints

Photographs and hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected. They will be treated in the same way as digital images.

At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste.

This code of practice will be reviewed annually to assess its implementation and effectiveness and it will be promoted and implemented throughout the Trust.

Appendix B - Privacy Impact Assessment

1. Who will be captured on CCTV?
Pupils, staff, parents / carers, volunteers, Governors and other visitors including members of the public etc.

2. What personal data will be processed?
Facial Images, behaviour, etc.

3. What are the purposes for operating the CCTV system? Set out the problem that the Trust is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

- To provide a safe and secure environment for pupils, staff and visitors;
- To assist with behaviour management and to ensure pupils take responsibility for their behaviour;
- To prevent the loss of or damage to the Trust buildings and/or assets; and
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

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?
School Business Manager; Headteacher/Principal of each school

6. Describe the CCTV system:

a. Fixed CCTV system with cameras located within the school grounds (internally and externally). The cameras are high specification to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained.
b. Cameras have been sited within the School grounds to avoid capturing images which are not necessary for the purposes of the CCTV system;
c. Signs indicating that CCTV is in operation are located at various locations within the site. These are located on the main entrances, within the car park and footpaths throughout school so that they are clearly visible to all stakeholders.

7. Set out the details of any sharing with third parties, including processors
CCTV footage maybe provided to external parties such as the Police, or through subject access requests. Careful consideration will be given to whether any provider is used in relation to the CCTV system and the access they might have to images.
The CCTV system is monitored by a third party monitoring company who have direct access to live images of the CCTV system once the system is armed on the schedule. All recording data is stored on the CCTV system itself, on individual hard drives located inside the unit.

8. Set out the retention period of any recordings, including why those periods have been chosen.
28 days retention. This allows a length of time to investigate any incidents whilst no burdensome on the system memory.

9. Set out the security measures in place to ensure that recordings are captured and stored securely.
CCTV footage is only accessible on one PC which is password protected.
Only Key individuals have access to this PC.
The footage is stored on the CCTV Server with no other access

10. What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

- Identification of an individual
- Loss of data if recordings disclosed to a third party (such as the police) if data not encrypted
- Misuse of data if accessed by non-authorised individual

11. What measures are in place to address the risks identified?

- Is it fair to record them in the way proposed?
  Yes, we have a duty of care to our pupils, staff and visitors and CCTV facilitates this
- How is the amount of data processed to be minimised?
  28 days retention period and only accessed by key individuals
- What are the risks of the system being accessed unlawfully?
  Low – password protected and only key individuals have access
- What are the potential data breach risks?
  CCTV footage released publicly without consent – loss of data.
- What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?
  Loss of data – Secure Encrypted USB to be used when transferring any data

12. 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?

CCTV Installation was prior to the formation of the Trust. Any changes will be approved by the AGB of each academy (each academy having parent governors).

13. When will this privacy impact assessment be reviewed?

As required or with any changes to CCTV system in any of the academies.

Approval:

This assessment was approved by the Data Protection Officer for Leger Education Trust:

DPO: Tim Pinto
Date: 12/10/2020
Reviewed: 13/10/2022

Appendix C – CCTV Release Request Form

Name:	Date:
Please provide a brief description of the CCTV footage including the date, time and location covered:	
Released by:	
I accept that the footage is supplied to me without prejudice. I understand that it was recorded on private premises and includes third parties. In accordance with the GDPR and Data Protection Act 2018 and in compliance with regulations laid down by the Information Commissioner, I will not publish, broadcast, undermine due confidence, nor otherwise cause any breach of the personal data, nor further process the data in a manner where it could affect the rights and freedoms of any other individual or groups of individuals. I understand that all relevant parties reserve the right to protection of the law and any breach could result in legal proceedings.	
Signed:	Date: