CCTV Policy and Procedures

Date: July 2021

Review date: July 2024

limetrust.london
Lime Trust c/o 70-72 New Road, Chingford, London E4 8ET
M: 07724 682 363 E: info@limetrust.london www.limetrust.london CN: 09297519

Introduction

The purpose of these Procedures is to regulate the use of CCTV and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Lime Trust, hereinafter referred to as 'the Trust Offices and Schools'.

The CCTV system is owned and operated by the Trust Offices and Schools, the deployment of which is determined by the Trust Offices and Schools senior leadership team.

These procedures follow the Information Commissioner's Office (ICO) 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data' (May 2015); the Data Protection Act (DPA) guidelines and the Trust Offices and Schools Data Protection Policy, both of which are held separately.

These Procedures will be subject to regular review to include consultation as appropriate with interested parties.

New CCTV systems will be introduced in consultation with staff, the Trust Offices and Schools senior leadership team, students and parents/carers. For this reason, the Trust / Academy will carry out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

Where systems are already in operation, their operation will be reviewed regularly in consultation with staff, the Trust Offices and Schools senior leadership team, students and parents/carers.

No Blame Culture

The Lime Trust believes in a no blame culture and will seek to use CCTV as a tool for organisational learning and to keep pupils and staff members safe.

CCTV will not be used for routine surveillance of any kind.

CCTV will only be accessed if a concern is raised for which CCTV may be able to provide clarification, or in order to provide training and support following a post-incident debrief (For example, if restrictive physical intervention has been used).

Statement of Intent

Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The Trust/Academy will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

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. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 30 days.

Exemptions

The use of surveillance systems for limited household purposes is exempt from the DPA e.g. a video of a child in a nativity play recorded for the parent/carer's own family use is not covered by the DPA.

The covert surveillance activities of public authorities (refer to Section 7) are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type of recording is covert and directed at an individual or individuals.

The use of conventional cameras (not CCTV) by the news media or for artistic purposes, such as for film making, are not covered by these procedures as an exemption within the Data Protection Act (DPA) applies to activities relating to journalistic, artistic and literary purposes.

Objectives of the CCTV scheme

The system comprises a number of fixed and dome cameras located around the both internally and externally for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external localities of the premises during both the daytime and hours of darkness. CCTV surveillance at the Trust / the Academy are intended for the purposes of:

- Protecting the Trust Offices / Academy buildings and assets, both during and after Trust Office / Academy hours
- Increasing the personal safety of staff, pupils and visitors
- Reducing the fear of crime
- Reducing the risk of bullying
- 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
- Protecting members of the public
- Ensuring that the Trust Offices and Schools rules are respected so that the Trust Offices and Schools can be properly managed
- Continually improving our use of Restrictive Physical Intervention (RPI), using a 'lessons learned' approach with leaders and staff

General Principles

The Trust as the corporate body has a statutory responsibility for the protection of its property and equipment as well providing a sense of security to its employees, students and visitors to its premises. The Trust owes a duty of care under the provisions of the Health and Safety at Work etc. Act, 1974 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the Trust community by integrating the best practices governing the public and private surveillance of its premises. The use of CCTV, and the associated images and any sound recordings is covered by the Data Protection Act 1998. These Procedures outline the Trust's use of CCTV and how it complies with the Act. The Trust will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

The Trust 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 continued use. The ICO 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Data,

May 2015 can be found on the ICO website.

The Chief Operating Officer for the Trust is responsible for all day-to-day data protection matters, and s/he will be responsible for ensuring that all members of staff and relevant individuals abide by these procedures, and for developing and encouraging good information handling within the Trust and Academies. The Lime Trust is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. Notification to the ICO is renewed annually.

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 operators are trained in their responsibilities under these

CCTV Procedures. Staff using the surveillance system or information have been trained to ensure they comply with these procedures. In particular, they have been made aware of:

- What the Trust's / Academy's arrangements are for recording and retaining information
- How to handle the information securely
- What to do if they receive a request for information, for example, from the police
- How to recognise a subject access request and what to do if they receive one

Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited e.g. monitoring of political or religious activities, or employee and/or student evaluations that would undermine the acceptability of the resources for use regarding critical safety and security objectives.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Trust including the Data Protection Policy and Behaviour Policy (incorporating Anti-Bullying and Harassment strategies) etc.

Our procedures for video monitoring prohibits monitoring based on the characteristic and classification contained in Equality and other related legislation, for example race, gender, sexual orientation, national origin, disability etc. The system is in place to monitor suspicious behaviour and not individual characteristics.

Video monitoring of public areas for security purposes is limited to uses that do not violate the reasonable expectation of privacy as defined by Law.

Consideration will be given to both staff and students regarding possible invasions of privacy and confidentiality due to the location of a particular CCTV camera or associated equipment. The Chief Operating Officer and Academy Lime Trusts will ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the Trust Offices and Academies and be mindful that no such infringement is likely to take place. The camera control will be monitored to ensure it is not in breach of the intrusion on intimate behaviour by persons in public changing and toilet areas.

Cameras will be used to monitor activities within the Trust offices and Academy car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the Trust's Trust Offices and School staff, pupils and visitors.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000 (RIPA).

The Chief Operating Officer and Academy Lime Trusts will approve any temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. (Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for criminal investigations).

When a zoom facility on a camera is being used, a second person will be present with the camera operator to guarantee that there is no unwarranted invasion of privacy.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the surveillance scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

CCTV Warning signs, as required by the ICO Code of Practice, have been placed at all access routes to areas covered by the Trust Offices and School CCTV – refer to Section 8.

Information obtained through the CCTV system may only be released when authorised by the Head teacher/Manager following consultation with the Chair of the Governing Body. Any requests for CCTV

recordings/images from the Police will be fully recorded. If a law enforcement authority is seeking a recording for a specific investigation, any such request made should be made in writing.

Justification for Use of CCTV

Visual Recording

The Data Protection Act requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the Trust / Academy needs to be able to justify the obtaining and use of personal data by means of a CCTV system by conducting a Privacy Impact Assessment (PIA) – refer to the Information Commissioner's Office 'Conducting Privacy Impact

Assessments' Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf . We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate and address a pressing need that we have identified. We have considered less privacy intrusive methods of achieving this need where possible.

The use of CCTV to control the perimeter of the Trust Offices and Academy buildings and entrances/exits for security purposes has been deemed to be justified by the Senior Leadership Team. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation for example.

Lime Trust makes provision for very vulnerable children and young people. The pupil groups at the Academies in the Trust include those with significant Social, Emotional and Mental Health needs. Sometimes, these young people exhibit behaviours that put themselves and others at risk. It has been demonstrated that there is a proven risk to safeguarding, health and safety and well-being of staff and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to installation of the system.

CCTV systems will not be used to monitor normal teacher/student classroom activity in Trust Offices and Schools.

Audio Recording

Not applicable at Lime Trust's operation of the System

Operations of the System

Control Room (Reception Area)

Viewing of live images on monitors in the Academies is restricted to the operator and any other authorised persons where it is necessary for them to see it. Monitors are located in Academy office areas and show staff, students and visitors in and around the Trust Offices and Academy, i.e. out of sight of the office area. These monitors have been positioned so that they are only visible to staff and members of the public are not allowed access to the area where they can view them.

Recorded images are viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy are restricted to authorised personnel:

- Lime Trust Leadership Team
- Academy Senior Leadership Team (Lime Trust, Deputy Lime Trust, School Business Manager)

CCTV is monitored centrally from the Academy Office area and cameras show images that could not be seen by the public from the main reception.

The School Business Manager / Senior Leader with responsibility for ICT and Site Manager will check and confirm the efficiency of the system and in particular that the equipment is recording properly and that cameras are functional.

Visitors and other contractors wishing to enter the Academy office area will be subject to particular arrangements. Academy Office staff must satisfy themselves over the identity of any visitors to the office and the purpose of the visit. Where any doubt exists access will be refused. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

If out of hours emergency maintenance arises, staff must be satisfied of the identity and purpose of contractors before allowing entry.

The Academy Office is not staffed out of hours and weekends so must be locked. During the working day when not staffed the office must be kept secured.

Other administrative functions will include maintaining video data and hard disc space, filing and maintaining occurrence and system maintenance logs.

Emergency procedures will be used in appropriate cases to call the Emergency Services.

Learning from CCTV

The Lime Trust policy is that RPI will only be used as an absolute last resort. It is only acceptable for staff to use RPI if the pupil is an immediate significant risk to the safety of themselves or others. Examples of when RPI would be appropriate are included in our Policy on RPI. Lime Trust leaders will, from time to time, review CCTV recordings following an event when RPI has taken place to see if there are any lessons to be learned and to support staff to improve practice. We believe that this supportive measure is proportionate and justified because it improves the culture of safeguarding at our schools, and acknowledges the additional vulnerabilities of our pupils, many of whom cannot let us know about their experiences of RPI themselves.

Siting of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. The Trust / the Academy have endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV video monitoring and recording of public areas in the Trust Offices and Academies may include the following

- **Protection of Trust Offices and Academy buildings and property:** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services.
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas.
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms.
- **Criminal Investigations (carried out by the Police):** Robbery, burglary and theft surveillance.

The following points were considered when the CCTV cameras were installed:

- Camera locations were chosen carefully to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.
- Where CCTV has been installed to deal with a specific problem, we have considered setting the system up so it only records during the time when the problem usually occurs.
- The cameras have been sited to ensure that they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- Cameras are suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- Areas are checked so that a fixed camera positioned in winter will not be obscured by the growth of plants and trees in the spring and summer.
- Cameras are sited so that they are secure and protected from vandalism.
- The system will produce images of sufficient size, resolution and frames per second.

Covert Surveillance

The Trust / the Academy will not engage in covert surveillance.

Certain law enforcement agencies may request to carry out covert surveillance on Trust Offices and Academy premises. Such covert surveillance may require a Court Order. Accordingly, any such request made by law enforcement agencies will be requested in writing. The covert surveillance activities of public authorities are not covered in this Policy as they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000. This type

of recording is covert and directed at an individual or individuals.

Notification – Signage

The Chief Operating Officer, Lime Trust of Senior Leader with responsibility for ICT within any Academy will provide a copy of the CCTV Policy on request to staff, pupils, parents/carers and visitors to the Trust Offices / Academy. This Policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use.

We must let people know when they are in an area where a surveillance system is in operation. The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as a simple website address, telephone number or email contact; and be an appropriate size.

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the Trust Offices and Schools property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour and bullying, for the safety of our staff and students and for the protection of Lime Trust Offices / Lime Academy XXX
This scheme is controlled by Lime Trust / Lime Academy XXX.
For more information Tel: XXX

All staff will be made aware of what to do or who to contact if a member of the public makes an enquiry about the surveillance system.

Storage and Retention of Recorded Images

Storage

Recorded material will be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. Recorded material is stored in a secure environment (Main office) with a log of access kept by the Headteacher.

Access to recorded material is restricted to the staff as outlined above. All recorded information is secure and where necessary, encrypted. Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. DVDs / Encrypted USBs will be stored in a secure environment with a log of access to DVDs / Encrypted USBs kept. Access will be restricted to authorised personnel as above. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

Supervising the access and maintenance of the CCTV System is the responsibility of the Associate Headteacher with responsibility for ICT and Site Services Manager. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above e.g. the Police, the Deputy Head teacher, the relevant Assistant Head, other members of the teaching staff, representatives of the DfE, representatives of the HSE and/or the parent of a recorded student. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

The Trust / the Academy will keep a record or audit trail showing how the information must be handled if it is likely to be used as evidence in court. Once there is no reason to retain the recorded information, it will be deleted. Exactly when we decide to do this will depend on the purpose for using the surveillance systems. A record or audit trail of this process will also be captured.

CCTV images are digitally recorded. It is important that the information can be used by appropriate law enforcement agencies if it's required. A written request, which must state the purpose of the request for transfer to DVD / USB must be made to the Chief Operating Officer or Lime Trust.

Retention

The Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. As a data controller, Lime Trust needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (30 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/ prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/ prosecution of that issue.

DVD Procedures / Encrypted USB

In order to maintain and preserve the integrity of the Data used to record events from the software and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- DVD / Encrypted USBs must be identified by a unique mark.
- Before using, each DVD / Encrypted USB it must be cleaned of any previous recording.

The controller shall register the date and time of DVD / Encrypted USB insert, including tape/encrypted USB reference.

A DVD / Encrypted USB required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure evidence DVD / Encrypted USB store. If a DVD / Encrypted USB is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence DVD / Encrypted USB store.

If the DVD / Encrypted USB is archived the reference must be noted.

Data may be viewed by the Police for the prevention and detection of crime, authorised officers of the Local Authority for supervisory purposes, authorised demonstration and training.

A record will be maintained of the release of Data to the Police or other authorised applicants. A register will be available for this purpose.

Viewing of Data by the Police must be recorded in writing and in the CCTV log book. Requests by the Police can only be actioned if they meet the legislative requirements of the Data Protection Act 2018 and General Data Protection Regulations.

Should a DVD / Encrypted USB be required as evidence, a copy may be released to the Police under the procedures described previously in this Code. Data will only be released to the Police on the clear understanding that the DVD / Encrypted USB remains the property of the Trust, and both the DVD / Encrypted USB and information contained on it are to be treated in accordance with this code. The Trust / Academy also retains the right to refuse permission for the Police to pass to any other person the DVD / Encrypted USB or any part of the

information contained thereon. On occasions when a Court requires the release of an original DVD / Encrypted USB this will be produced from the secure evidence DVD / Encrypted USB store, complete in its sealed bag.

The Police may require the Trust Offices / Academy to retain the stored Data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Head teacher. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

Access

Digitally captured images and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to DVDs / Encrypted USBs will be maintained.

Access to CCTV system and stored images will be restricted to authorised personnel only, i.e. the Chief Operating Officer / Lime Trust.

Disclosure of Images

There will be no disclosures of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Trust and Academies where these would reasonably need access to the data (e.g. investigators). In relevant circumstances, CCTV footage may be disclosed:

- To the Police where the Trust /Academy is required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal / anti-social behaviour is taking place on the Trust Offices and Academy's property, or
- To the HSE and / or any other statutory body charged with child safeguarding; or
- To assist the Chief Operating Officer / Headteacher in establishing facts in cases of unacceptable student behaviour, in which case, the parents/carers will be informed. The data may be used within the Trust Offices and Academy's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures, or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to the Trust Offices and Academies; or
- The individuals (or their legal representatives) subject to a court order; or
- To the Trust's insurance company where the insurance company requires evidence in order to pursue a claim for damage done to the insured property

Only authorised and trained staff are allowed to make external disclosures of CCTV footage, i.e. Chief Operating Officer / Headteacher.

Data will never be placed on the internet and will not be released to the media. Information may be released to the media for identification purposes but this must NOT be done by anyone other than a law enforcement agency.

Once we have disclosed information to another body, such as the police, they become Data Controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures.

Requests by the Police

Information obtained through video monitoring will only be released when authorised by the Chief Operating Officer / Headteacher following consultation. If the Police request CCTV images for a specific investigation, any such request made by the Police should be made in writing.

Subject Access Requests

Staff involved in operating the surveillance system have been trained to recognise a subject access request. A

log of requests received will be kept and how they were dealt with. As mentioned, each DVD / Encrypted USB must be identified by a unique mark to allow easy retrieval.

On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image / recording exists, i.e. has not be deleted and provided also that an exemption / prohibition does not apply to the release. Where the image / recording identifies another individual, those images may only be released where they can be redacted /anonymised so that the other person is not identified or identifiable. Where a subject access request is received for surveillance footage or other information, we are required to provide a data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. This must be done by supplying them with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply.

The first is where the data subject agrees to receive their information in another way, such as by viewing the footage. The second is where the supply of a copy in a permanent form is not possible or would involve disproportionate effort. The ICO's Subject Access Code of Practice makes clear this provision is only likely to be relevant in exceptional cases. If the data subject refuses an offer to view the footage or the data subject insists on a copy of the footage, then the Lime Trust / Academy must consider ways in which the data subject can be provided with this information.

The Trust and it's academies will always first attempt to provide the footage to the individual, or invite the data subject to a viewing if they consent to this.

If an individual agrees to a viewing of the footage but subsequently asks for that footage, it may be necessary, or at least good practice, to provide this footage where possible.

To exercise their right of access, a data subject must make an application in writing to the Data Protection Officer / Headteacher. The Trust Offices and Academies will respond to requests **within 30 days** of receiving the written request and fee.

Requests for Data Subject Access should be made on an application form available from the Trust Offices and Schools Office (refer to the Trust Offices and Schools Data Protection Policy for further details).

A person should provide all the necessary information to assist the Trust in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the Trust / Academy. The Trust / Academy reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

In giving a person a copy of their data, the Trust may provide a still/series of still pictures, a DVD or encrypted USB with relevant images. However, other images of other individuals will be obscured before the data is released.

For further information on subject area requests, refer to the ICO's 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

Freedom of Information

Lime Trust may receive requests under the Freedom of Information (FOI). We have a member of staff who is responsible for responding to freedom of information requests, and understands the Trust's responsibilities. The Trust must respond within 20 working days from receipt of the request.

Section 40 of the FOIA contain a two-part exemption relating to information about individuals. If the Trust receives a request for surveillance system information, we will consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA. Instead this request should be treated as a data protection subject access request as explained above.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles.

In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be

disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the Data Protection Act.

Security Companies

The Trust CCTV system is controlled by a security company, XXXX, contracted by the Trust/Academy. The following applies:

The Trust / Academy has a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply. The written contract also states that the security company will give the Trust Offices and Academies all reasonably assistance to deal with any subject access requests made under the Data Protection Acts 1988 and 2003 which may be received by the Trust / Academy within the statutory time-frame (maximum 30 days).

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients). The Data Protection Act place a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company have been made aware of their obligations relating to the security of data. See Content of the Service Agreement for further guidance.

Breaches of the Procedures (including security breaches)

Any breach of these procedures by Trust staff will be initially investigated by the Chief Operating Officer / Data Protection Officer, in order for him/her to take the appropriate disciplinary action.

Any serious breach of the procedures will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

Information obtained in violation of these procedures may not be used in a disciplinary proceeding against an employee of the Trust, or a pupil.

Monitoring and Review

Routine performance monitoring, including random operating checks, may be carried out by the Headteacher / School Business Manager / Site Services Manager.

These procedures will be regularly reviewed, either by a designated individual within the Trust Offices and Academies or by a third party. This is to ensure the standards established during the setup of the system are maintained.

Similarly, there will be a periodic review, at least annually, of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it should be stopped or modified. Refer to Appendix A, for a sample Annual Review Checklist.

The review will take into account the following:

- Is it addressing the needs and delivering the benefits that justified its use?
- Is information available to help deal with queries about the operation of the system and how individuals may make access requests?
- Does the information include our commitment to the recommends in the ICO Code of Practice and include details of the ICO if individuals have data protection compliance concerns?
- Is a system of regular compliance reviews in place, including compliance with the provision of the ICO Code of Practice, continued operational effectiveness and whether the system continues to meet its purposes and remains justified?
- Are the results of the review recorded, and are its conclusions acted upon?

The periodic review will also ensure all information is sufficiently protected to ensure that it does not fall into

the wrong hands. This will include technical, organisational and physical security. For example:

- Sufficient safeguards are in place to protect wireless transition systems interception.
- The ability to make copies of information is restricted to appropriate staff
- There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.
- Where information is disclosed, it is safely delivered to the intended recipient, e.g. by Royal Mail Special Delivery if posted or identification verified and receipt signed for if collected in person.
- The Control Room and room where information is stored is secure.
- Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information
- Staff have been made aware that they could be committing a criminal offence if they misuse surveillance system information
- The process for deleting data is effective and adhered to
- If there have been any software updates (particularly security updates) published by the equipment's manufacturer that have been applied to the system.

Complaints

- Any complaints about the Trust's CCTV systems should be addressed to the Chief Operating Officer / Headteacher
- Complaints will be investigated in accordance with these Procedures.

Further Information

Further information on CCTV and its use is available from the following:

- The Information Commissioners Office 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information, 2017 https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
- The Information Commissioners Office (ICO) Website https://ico.org.uk
- The Information Commissioners Office (ICO) 'Conducting Privacy Impact Assessments' Code of Practice' https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- The Information Commissioners Office (ICO) 'Subject Access Code of Practice' https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 1998 https://ico.org.uk/for-organisations/guide-to-data-protection
- Lime Trusts' Data Protection Policy