istitutomarangoni

ISTITUTO MARANGONI LONDON
CCTV POLICY

September 2021

istitutomarangoni

Version Control Statement

Version	1.0		
Document title	Istituto Marangoni London CCTV Policy		
Document approved by	Prevent Working Group (March 2021)		
Approval date	7 September 2021		
Date for review	September 2022		
Amendments since approval	**Detail of revision**	**Date of revision**	**Revision approved by**
	Added section 1.2	12/08/2021	London School Board

0. TABLE OF CONTENT

1. Policy Statement

1.1 Istituto Marangoni London believes that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by surveillance systems are personal data which are processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, relating to their personal data, are recognised and respected.

1.2 This policy covers Employees, Faculty, Students, Visitors and anyone else who enters School property.

1.3 This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

2. Definitions

2.1 For the purposes of this policy, the following terms have the following meanings:

CCTV: fixed and domed cameras designed to capture and record images of individuals and property.

Data: information which is stored electronically, in respect of CCTV, this generally means video files or images.

Data Subjects: all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Personal Data: data relating to a living individual who can be identified from that data (or other data in our possession). This includes video images of identifiable individuals.

Data Controllers: the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the data controller of all personal data used in our business for our own commercial purposes.

Data Users: those of our employees whose work involves processing personal data. This includes those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Privacy Standard.

Data Processors: any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Processing: any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Recordings: CCTV Records and Stores data on an encrypted local drive

Extracted Recordings: Recordings may be extracted with reasonable cause

Surveillance Systems: any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition

(ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

3. ABOUT THIS POLICY

3.1 We currently use CCTV cameras to view and record individuals on and around our premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with Data Protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

3.2 We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the legislation. We are a data controller and we have registered our use of CCTV with the Information Commissioner. We are committed to complying with our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

3.3 This policy covers all staff, employees, students and other individuals working and/or visiting our premises.

3.4 This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this policy at any time without consultation. The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

3.5 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

4. Personnel Responsible

4.1 The ICT Manager has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. The Facilities Operator has day-to-day operational and management responsibility for deciding what information is extracted from the recordings, how it will be used and to whom it may be disclosed. The ICT Manager has responsibility of data storage methods.

4.2 Responsibility for keeping this policy up to date has been delegated to the ICT Manager.

5. Reasons for the Use of CCTV

5.1 We currently use CCTV around our site as outlined below. We believe that such use is necessary for legitimate business purposes, including:

5.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

5.1.2 for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;

5.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime;

5.1.4 to assist in day-to-day management, including ensuring the health and safety of staff and others;

5.1.5 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and

5.1.6 to assist in the defence of any civil litigation, including employment tribunal proceedings.

This list is not exhaustive and other purposes may be or become relevant.

6. Monitoring

6.1 Exterior CCTV monitors both the main entrance and secondary exits in the back of the building. Internal CCTV monitors public spaces inside the building. This includes open space, reception area, corridors and stairwells. These cameras are continuously recording 24 hours in the day.

6.2 Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

6.3 Surveillance systems will not be used to record sound.

6.4 Images are monitored by authorised personnel during working hours only. Or when needed outside of working hours via a remote access. Viewed by authorised members of staff only, in both cases.

6.5 Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

7. How We Will Operate Any CCTV

7.1 Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

7.2 Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

7.3 We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

8. Use Of Data Gathered By CCTV

8.1 In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

8.2 Given the large amount of data generated by surveillance systems, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

8.3 We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

9. Retention Of Data Gathered By CCTV

9.1 Data recorded by the CCTV system will be stored digitally using a local DVR system stored on an encrypted hard drive. Data from CCTV cameras may be extracted but in the event of a confirmed security threat or incident. The Extracted data will not be retained indefinitely and will be deleted once there is no reason to retain the extracted information. Exactly how long images will be retained for will vary according to the purpose for which they are being extracted. For example, where images are being extracted for crime prevention and investigation purposes,

data will be kept long enough only for incidents to come to light and be concluded. In all other cases, recorded images are automatically deleted after 2 months by the automated recording system.

9.2 At the end of their useful life, all images stored in whatever format will be erased permanently and securely.

9.3 Recordings are never printed into hard copies or saved on discs or portable hard drives.

10. Use Of Additional Surveillance Systems

10.1 Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a Data Privacy Impact Assessment (DPIA).

10.2 A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

10.3 Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

10.4 No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

11. Covert Monitoring

11.1 We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

11.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the ICT Manager. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers will always be a primary consideration in reaching any such decision.

11.3 Only limited numbers of people will be involved in any covert monitoring.

11.4 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.[AS3]

12. Ongoing Review Of CCTV Use

12.1 We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction.

13. Requests For Disclosure

13.1 We may share data with other groups or companies where we consider that this is reasonably necessary for any of the legitimate purposes set out above in Paragraph 5.1. We will only share extracted recordings to companies that are under contractual obligation to provide Security Services to the company.

13.2 No images from our CCTV cameras will be disclosed to any other third party, without express permission being given by the School Director. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

13.3 In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

13.4 We will maintain a record of all disclosures of CCTV footage subject to document retention guidelines.

13.5 No images from CCTV will ever be posted online or disclosed to the media.

14. Subject Access Requests

14.1 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (data subject access request). A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing.

14.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

14.3 We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

15. Complaints

15.1 If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to the ICT Manager in the first instance.

15.2 Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure.

16. Requests To Prevent Processing

16.1 We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances, to prevent automated decision making (see Articles 21 and 22 of the GDPR). For further information regarding this, please contact the ICT Manager.