EMMANUEL SCHOOLS FOUNDATION

Closed Circuit Television (CCTV) Policy

Last review: February 2022
Approved by Trustees: Feb 2022
Next review: February 2023

Table of Contents

CCTV POLICY

General Statement

This policy is concerned with the use and governance of surveillance technology, and the processing of Personal Data which has been collected by using surveillance technology. The policy is written in accordance with various Data Protection legislation, which includes, but is not limited to, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), and the Information Commissioner's Office's (ICO) surveillance code of practice.

Queries about this policy should be directed to Emmanuel School Foundation's (Trust")) Data Protection Officer.

Scope

This policy applies to all students, Trust employees, any authorised agents working on behalf of the Trust, including temporary or agency staff, governors, volunteers, and third-party contractors and any other individual visiting a Trust site.

Surveillance is the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. The Trust uses surveillance in the context of CCTV and e-monitoring software.

The Trust does not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV Purpose

The Trust and schools within the Trust may operate CCTV systems for the following purposes: -

- For the safety and security of the school and its students, staff, visitors, volunteers, governors, trustees and any other individual visiting a Trust site;
- To protect the school 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;
- To assist in the investigation of accidents, incidents and near misses

Planning CCTV Systems

Any new implementation of CCTV systems will employ the concept of 'privacy by design' which will ensure that privacy implications to data subjects will be considered before any new system is procured/installed. The prescribed method for this is through the completion of a Data Protection Impact Assessment (DPIA).

The Trust has various statutory responsibilities to protect the privacy rights of data subjects. During any planning phase the Trust and its school will consider:

- The purpose of the system and any risks to the privacy of data subjects.

- That there are statutory requirements placed on the location and position of cameras. This means that cameras must be positioned to meet the requirement(s) of the intended purpose(s) and not exceed the intended purpose(s).
- The obligation to ensure that the CCTV system can meet its intended purpose(s) also means that the system specification must be such that it can pick up any details required for these aims. For example, the system must record with sufficient resolution to perform its task.
- The system must also have a set retention period. The Trust has the ability to delete this information prior to the set retention period in order to comply with the rights of data subjects.
- That the Trust will need a level of access to the system and there will need to be the option to provide other agencies (such as law enforcement agencies) with specific footage if requested. If a data subject is captured and recorded by the system, then that individual also has the right to request a copy of that footage under subject access provisions.

The school will ensure that a contract will be agreed between the Trust (as Data Controller) and the CCTV system provider. Consideration will also be given as to whether there are any joint data controller arrangements where the system is shared with another organisation. Data Processing clauses will be included within any written contract should the Trust choose to work with a CCTV service provider who will be processing (e.g. monitoring, storing, accessing) the data on behalf of the school.

CCTV Privacy Notices

The processing of personal data requires that the individuals the data relates to (in this case any individuals captured by the CCTV) are made aware of the processing. Therefore, the use of CCTV systems will be visibly signed. The signage will include the purpose for the system (e.g. the prevention or detection of crime), the details of the organisation operating the system and who to contact about the system (including basic contact details). The signage must be clear enough that anyone entering the recorded area will be aware that they are being recorded.

A more detailed Privacy Notice for the use of CCTV must be maintained with the intention of informing data subjects of their rights in relation to surveillance data. This will be available on the school (if applicable) and Trust websites.

Access to CCTV Recordings

CCTV footage will only be accessed to comply with the specified purpose and the footage will only be examined to meet one of the purposes described above.

The CCTV system will have a nominated Information Asset Owner (IAO) on site who will be responsible for the governance and security of the system, the Trust will keep a record of the IAO on each site and schools will notify the Trust DPO of any changes to this person. The Information Asset Owner will authorise appropriate staff of the Trust employed at the school to access CCTV footage either routinely or on an ad-hoc basis and ***in compliance with the school's CCTV Procedure***.

CCTV Footage Disclosures

A request by individuals for CCTV recordings that include footage of them is regarded as a subject access request (SAR). For more information on the right of access for individuals captured on CCTV, refer to the Trust's Data Protection Policy.

If the Trust/School receives a request from another agency (for example a law enforcement agency) for CCTV recordings, then it will confirm the following details with that agency:

- the purpose of the request,
- that agency's lawful basis for processing the footage,
- confirmation that not receiving the information will prejudice their investigation,
- whether the Trust/School can inform the data subject of the disclosure, and if not, the reasons for not doing so.

The Trust/School will liaise with its appointed Data Protection Officer/local Data Champion should it have any concerns about such requests.

Review of CCTV

CCTV systems should be reviewed within the same timeline for the Trust Information Security Policy to ensure that systems still comply with Data Protection legislation and national standards.

The Information Asset Owner should use the checklist included in Appendix 1 of this policy to complete this review. It is the responsibility of the Information Asset Owner on site to ensure reviews are completed and evidence of those reviews taking place are maintained and shared appropriately with the Trust DPO and the LGB.

E-Safety Monitoring

The Trust operates e-safety monitoring software systems in order to safeguard students and inform IT staff when any student searches for or looks at inappropriate or malicious content. Software is also used to ensure students are "on task" within lessons. This is a form of non-covert surveillance processing. The use of E-Safety Monitoring software is included in the Privacy Notice for the school where relevant and is covered in more detail in the relevant Trust policy.

Complaints

Complaints by individuals about the use of surveillance systems, or the way surveillance data is processed, should be treated as a data protection concern and the school's data protection officer should be made aware.

The Trust's Data Protection Officer is Christine Taylor who may be contacted at ctaylor@esf-mail.org.uk

Records of Processing

The Trust has a duty under Article 30 of the GDPR to ensure that all instances of data processing activity is recorded for regulatory inspection where required. The Trust requires schools to maintain an information asset register to fulfil this requirement on behalf of the Trust.

Each Trust school will therefore ensure that the use of surveillance systems is recorded on their information asset register. This should detail each separate surveillance system in use.

Related Documents

Employees including, but not limited to, the IAO and the DPO, who are responsible for planning, maintaining, or reviewing the implementation of a surveillance system are encouraged to read the following related documents prior to implementation:

- ICO Surveillance Code of Practice (External Link)
- The Trust's Data Protection Impact Assessment (DPIA) Template available from the Trusts DPO

Appropriate training will be arranged by the Trust for the IAO in each school and for the Trust DPO.

This policy represents the Emmanuel Schools Foundation's Code of Practice for the ethical operation of its CCTV system. The CCTV policy is intrinsically linked to the Trust's Information Security Policy and each Trust school's Safeguarding Policy and should be reviewed with these in mind.

Code of Practice

In recognition of this policy, the Trust will ensure:

- The CCTV system is designed and installed by a suitably approved National Security Inspectorate 'NSI' contractor and will conform to the NSI code of practice.
- http://www.nsi.org.uk/wp-content/uploads/2012/10/NCP-104.3-Code-of-Practice-Design-Installation-and-Maintenance-CCTV-Nov-2017.pdf
- CCTV cameras are only installed to appropriate locations where there is an evidentiary need for this data
- External CCTV cameras will not record images beyond the boundary of the site.
- Rooms where CCTV is viewed are always kept secure.
- The CCTV system is operated in an ethical manner in accordance with the ICO CCTV code of Practice.
- Downloaded CCTV footage will be kept for a maximum of 14 days and then deleted.
- Footage that is deemed necessary for further investigation or legal purposes can be stored beyond the 14 days. This needs to be requested of and then approved by the IAO.
- CCTV footage stored beyond 14 days will be regularly reviewed for its currency and continued purpose and will be securely disposed of as necessary.

This policy should be read in conjunction with:

- ESF Information Security Policy
- School specific safeguarding policies
- ESF Data Protection Policy
- ESF Document Management Records and Policy Schedule
- ESF E-safety Policy
- ESF Privacy Notices

Appendix 1 – Surveillance System Checklist

To be completed for the School Information Asset Owner

School Name: _____

Name and Description of Surveillance System:		
The purpose and requirements of the system are addressed by the system (I.e. the cameras only record required information)	**YES**	**NO**
	Notes:	
The system is fit for purpose and produces clear images of adequate resolution.	**YES**	**NO**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**YES**	**NO**
	Notes:	
Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	**YES**	**NO**
	Notes:	
There are visible signs appropriately placed showing that CCTV is in operation. These signs include: ▪ Who operates the CCTV, ▪ Their contact details, ▪ What the purpose of the CCTV is.	**YES**	**NO**
	Notes:	

CCTV recordings are securely stored and access limited.	**YES**	**NO**
	Notes:	

The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information (SAR).	**YES**	**NO**
	Notes:	
The system has a set retention period. This retention period is only long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information is deleted	**YES**	**NO**
	Notes:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure of data subjects.	**YES**	**NO**
	Notes:	
All operators have been authorized by the Information Asset Owner (IAO) and have sat and passed their mandatory Trust data protection training.	**YES**	**NO**
	Notes:	
This system has been declared on the corporate register of	**YES**	**NO**

surveillance systems.	**Notes:**

Checklist Completed by: Name: Job Title: Date:	**Checklist Reviewed and Signed by (School Information Asset Owner):** Name: Job Title: Date:

To be shared annually with the Trust DPO and with the LGB