



**Inspiring Futures  
Through Learning**

Inspiring Futures Through Learning

CCTV Policy

April 2021 to April 2023

*At Inspiring Futures through Learning, we are driven by our pursuit of excellence every day. We have high expectations of learning, behaviour and respect for every member of our community. We create independent, articulate thinkers and learners who have confidence in, not only their individual ambitions, but also those of the Academy and The Trust as a whole. We have collaboration at the heart of everything we do and our vision is to nurture exciting, innovative, outstanding Academies who embrace change and provide a world-class education for all it serves.*

**\*Including all IFtL Schools, Milton Keynes Teaching School Alliance and Two Mile Ash Initial Teaching Training Partnership**

<b>Policy name:</b>		CCTV Policy
<b>Version:</b>		V2
<b>Date relevant from:</b>		April 2021
<b>Date to be reviewed:</b>		April 2023 <i>This policy will be reviewed every two years unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this Policy.</i>
<b>Role of reviewer:</b>		IFtL Head of Operations
<b>Statutory (Y/N):</b>		Y
<b>Published on website*:</b>		3C

<b>Policy level**:</b>	1
<b>Relevant to:</b>	All employees through all IFtL schools and departments
<b>Bodies consulted:</b>	
<b>Approved by:</b>	IFtL Finance and Resources Committee
<b>Approval date:</b>	4 <sup>th</sup> May 2021

**Key:**

**\* Publication on website:**

IFtL website		School website	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

**\*\* Policy level:**

1. Trust wide:
  - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
    - o *Approved by the IFtL Board of Trustees.*
2. Trust core values:
  - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore form the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
    - o *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
    - o *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*
3. School / department policies
  - These are defined independently by schools / departments as appropriate
    - o *Approved by school / department governance bodies.*

## Introduction

*This policy takes into account the requirements of the GDPR and the Data Protection Act 2018 and is written in accordance with the guidance in the CCTV Code of Practice issued by the Information Commissioner's Office.*

CCTV systems are in use in many schools across the country. Within IFtL schools, these systems are installed for the purposes of monitoring school buildings in order to provide a safe and secure environment for pupils, staff and visitors.

They are also used to prevent loss or damage to school property, to assist in the prevention and detection of crime and to assist law enforcement authorities in apprehending or prosecuting offenders.

Schools are responsible for managing their CCTV systems but must do so in line with this policy.

Overarching responsibility lies with the Trust and, as such, the Trust are registered with the ICO as the data controller.

All authorised operators of the CCTV system are bound by this policy and should ensure that they are familiar with its contents.

Misuse of CCTV systems could constitute a criminal offence. Any staff member breaching this policy may be subject to disciplinary action.

## New Installations

Where schools do not already have CCTV and wish to install a system, a Data Protection Impact Assessment **MUST** be carried out at the planning stage before any new system is designed.

As required by the ICO, privacy by design must be used to ensure that the system is compliant and that and impact on the rights and freedoms of individuals has been appropriately considered during the design stage.

## Viewing and Recording Images

Images are generally monitored live from the main school office and/or from the offices of

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



senior leaders. Schools should undertake an assessment of where live images may be required to be viewed and document the locations in the template at Appendix 1. Monitors should be placed in such a way that live footage is not viewable to visitors wherever possible (particularly where internal cameras are in operation around school). Recorded footage should only be accessed when an event occurs that requires the footage to be checked.

When accessing recorded footage, extra care should be taken that this is carried out in a secure location to ensure that only those authorised to view recordings are able to see the footage.

## Camera Positioning

Cameras must be positioned to ensure that they cover the areas relevant to the purpose of the system. Appropriate care must be taken to ensure that reasonable privacy expectations are not violated. For example, cameras should never be placed in toilets or in changing rooms nor should they be fitted in any area where staff have a reasonable expectation of privacy.

Every effort must be taken to ensure that cameras do not infringe on other properties outside of the school perimeter. Where neighbouring properties are overlooked, the system manager should investigate whether technical measures such as privacy filters can be implemented to block the view of such properties electronically.

CCTV camera locations should be clearly visible and known to staff, particularly in relation to internal cameras or cameras that cover external work areas. It is good practice to have a 'map' of your CCTV system available showing camera positioning and highlighting the areas that each camera covers. Internal cameras should have signage present within the area that the camera is placed to ensure that it is obvious to people in the area that a camera is present.

Appropriate signage must be displayed at all entrances, including gates, informing people that the area that they are entering is monitored by CCTV cameras.

CCTV will not be placed in classrooms or any internal areas, except for circulation or reception areas, without a documented assessment and a consultation exercise with stakeholders. (CCTV does not include systems that monitor teaching, such as IrisConnect, for example. These systems are not fixed and are designed to improve teaching and learning and, while a DPIA is required for their use, they do not fall within the remit of this policy).

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



In exceptional circumstances, where there are grounds to suspect serious misconduct or where suspected illegal activity is taking place, covert monitoring may be considered. Any covert monitoring must be discussed with the Trust's senior management prior to being undertaken and a documented audit trail must be retained showing why the decision to implement this has been taken.

Covert monitoring must cease on completion of the investigation for which it was implemented.

Covert monitoring must never take place in areas that are reasonably expected to be private such as toilets, for example.

Covert monitoring is a last resort and will only be authorised if no other reasonable means of achieving the same outcome are available.

## **Recording of Sound**

Cameras that are capable of recording audio as well as video should, generally speaking, have the sound recording functionality disabled.

Where schools wish to use the sound recording facility, a privacy impact assessment should be undertaken and a comprehensive justification of why sound is being recorded should be documented and kept on file. Explicit signage should be displayed informing people within the area covered that sound recording is in use as part of the CCTV system.

This process should be reviewed annually.

## **Storage and Retention of Images**

Recorded data will only be kept for as long as necessary. The trust recommends systems that automatically overwrite data and a retention period of 30 days.

Where images are required to be kept for longer, for evidential reasons for example, the images should be transferred onto a secure storage media with appropriate security in place to protect the stored images from unauthorised access.

Adequate security must be in place to ensure that images are safe from unlawful or inadvertent disclosure.

These could include;

- Locating CCTV systems in locked, restricted access areas
- Encrypting or password protecting access to systems
- Prevention of copying of images by unauthorised staff

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



Part of the maintenance checks of the system should include a check of logs to detect any unauthorised activity.

## **Subject Access Requests**

Individuals have the right to request copies of data that you hold about them. This includes CCTV recordings.

Where an individual wishes to make a subject access request, please refer to the Subject Access Request Policy. All requests should, ideally, be made in writing and should include sufficient information to enable the footage to be identified. For example, date, time and location of the footage. Where requests are not made in writing, we still have a legal obligation to treat such requests as if they had been made in writing. Schools should record all details in their system for managing SARs including details of the date of the request, the process followed to vet the footage for release, who viewed the images through this process and whether footage was provided, to whom, in what format and when it was supplied.

Where footage only contains images of the person requesting the footage, schools must release the data in line with our subject access request policy.

Where footage contains images of other persons, the following should be considered;

- Can the footage of other persons be blurred or otherwise obscured?
- Can the consent of the other persons be obtained prior to release?
- Would it be reasonable in the circumstances to disclose the footage regardless of consent or the inability to redact?

Schools reserve the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or where it may jeopardise an ongoing investigation.

## **Disclosure to Third Parties**

Data will not be disclosed to third parties unless permitted by data protection legislation, required by law, or in order to undertake an investigation where access might reasonably be required. This disclosure may be to the police or to other authorised agencies.

CCTV images can only be released for reasons in line with the purposes for which the system is in place.

Requests made by law enforcement agencies must follow the same protocol as subject access requests. Details of what footage is required and what the footage is required for

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



must be provided in order to enable a decision to be made as to whether third party images can legally be disclosed.

Specifics of any alleged offences are not required but enough detail to enable a decision to be made should be provided.

Where a court order is granted for disclosure of CCTV images, this should be complied with, but careful consideration must be given to exactly what the court order is requesting. Please contact the Trust's data protection officer for further guidance on this.

Persons appropriately trained in the retrieval and transfer of images should be available on-site so that the task of finding and retrieving such images can be carried out in a timely manner. This generally means that several members of staff should be trained in this procedure.

A log should be kept of all such disclosures which includes the detail of what was disclosed. A copy of video footage disclosed should be retained securely by the school for a period of one year following the conclusion of matters arising (such as court proceedings or disciplinary action) unless legislation requires footage to be kept for a longer period.

Data may also be used by the school in its own grievance and disciplinary procedures, subject to the usual confidentiality procedures surrounding such procedures.

## Complaints

Complaints should be made, in the first instance, to the school's headteacher or to the data protection officer at the Trust.

You also have the right to complain to the Information Commissioner at <https://ico.org.uk/concerns/>

## Further Reading

Please refer to the ICO's CCTV Code of Practice for further guidance at [cctv-code-of-practice.pdf \(ico.org.uk\)](#)

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



**Appendix 1: School Specific Information and checklist – All schools MUST complete this page**

Please fill this in with your school specific information. A check should be made annually to ensure that you remain compliant.

Where is your DVR (CCTV Recorder) located?	
Is this location kept secure or are other steps taken to ensure the security of the system?	
Who is the designated CCTV system manager?	
Who are the authorised operators for the CCTV system?	
Who is the person with responsibility for day-to-day operation of the system?	
Which locations have been identified as requiring live monitoring of images?	
Who are the individuals authorised to access and view recorded images from the system? (include people above if authorised)	
Does your CCTV have sound recording enabled?	
Are the images clear and stable?	
Are the cameras sited so as not to infringe on other people’s privacy?	
Is there correct signage in place at the appropriate locations?	
Are contact details stated on the signage as required by law?	
For how long does your system store recorded images?	
Do the images self-erase or is there a process in place to ensure retention and deletion periods are adhered to?	
Is someone in the school aware of the procedure for dealing with requests to access the images?	
Are weekly checks undertaken to ensure the images are good quality and stable and that the system is operating as designed – Who carries this out?	

Check carried out by:	
Date:	
Date for review:	
Reviewed (date):	

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*





Reviewed by:	
Reviewed (date):	
Reviewed by:	
Reviewed (date):	
Reviewed by:	
Reviewed (date):	
Reviewed by:	

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



## Appendix 2: Signage

It is a requirement of the Data Protection Act, to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

**The CCTV sign should include the following:**

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for enquiries
- A pictorial representation similar to the one shown below



*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



### Appendix 3: Camera Assessment

Where a new CCTV system is being installed, a full Data Protection Impact Assessment must be carried out. Where a new camera is to be added to an existing system, an evaluation of the potential risks should be carried out and the results documented.

An example assessment form is shown below.

Where is the new camera to be added?	
Why is the additional camera required?	
Will the captured images be treated any differently to the existing recorded images within the system?	
What do you hope to achieve by adding this camera?	
Does the placing of the camera impact on any areas where there may be a reasonable expectation of privacy?	
Does the addition of this camera add any risk to the rights or freedoms of individuals within this area?	
If any risks have been identified, are you able to reduce the risk?	
Does the lawful basis for processing this information differ from the rest of the system?	
Has the data protection officer been consulted about this proposal?	
Are you satisfied that the addition of this camera is a reasonable measure to achieve the outcomes required and that any risks to the rights or freedoms of individuals have been considered and, where appropriate, steps taken to mitigate?	
Addition approved by (Headteacher):	
Sign	Print: <span style="float: right;">Date:</span>

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



## Appendix 4: DPIA Template for CCTV System

Who will be captured on CCTV?

[Pupils, staff, parents / carers, volunteers, governors and other visitors including members of the public etc]

What personal data will be processed?

[Facial images, behaviour, sound, etc]

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

[Prevention or detection of crime etc]

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]

Who is/are the named person(s) responsible for the operation of the system?

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



Describe the CCTV system, including:

- a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained
- b. siting of the cameras and why such locations were chosen
- c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system
- d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen
- e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

Set out the details of any sharing with third parties, including processors

[Police, subject access, etc. Careful consideration should be given to whether any provider is used in relation to the CCTV system and the access they might have to images. Will those processors send this data outside of the EEA, for example for storage in a cloud based system?]

Set out the retention period of any recordings, including why those periods have been chosen

Set out the security measures in place to ensure that recordings are captured and stored securely

*IFTL is a trust established by educationalists, with education and improving outcomes for children at the heart of all we do.*



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

For example:

- Is it fair to record them in the way proposed?
- How is the amount of data processed to be minimised?
- What are the risks of the system being accessed unlawfully?
- What are the potential data breach risks?
- What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?

What measures are in place to address the risks identified?

Consider the design of the system, security protocols, policies, training

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?

When will this privacy impact assessment be reviewed?



**Approval:**

**This assessment was prepared by**.....

**And agreed by (HT/Principal)**.....

**On (date)**.....

**This assessment was approved/rejected by the Data Protection Officer:**

**DPO** .....

**Date** .....

**Additional Comments by DPO;**

