HLC CCTV Policy

"Belong, Respect, Inspire, Succeed, Enjoy"

This policy was created on	13th March 2024
This policy was updated on	7th October 2025
The policy is to be reviewed on	October 2027
Created By	Chris King

Our Community, Our School

HADLEY LEARNING COMMUNITY

Contents

Statement of Intent

1. Legal Framework
2. Definitions
3. Roles and Responsibilities
4. Purpose and Justification
5. The Data Protection Principles
6. Objectives
7. Security
8. Privacy by Design
9. Code of Practice
10. Access
11. Storage and Retention
12. Monitoring and Review
13. Notification and Signage
14. Appendix 1. Internal Access Protocols
15. Appendix 2: CCTV Data Release Request – Internal
16. Appendix 3: CCTV Subject Access Request Form
17. Appendix 4: Camera Locations
18. Appendix 5: Privacy Impact Assessment (PIA)

Statement of Intent

At Hadley Learning Community, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members, and to monitor any unauthorised access to our site.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with all data protection legislation, including the Data Protection Act 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy.

1. Legal Framework

1.1. This policy has due regard to legislation and statutory guidance, including, but not limited to the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Protection of Freedoms Act 2012 (Part 2 – CCTV & ANPR)
- Human Rights Act 1998
- European Convention on Human Rights
- Equality Act 2010
- Children Act 1989
- Children Act 2004
- School Standards and Framework Act 1998
- Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

1.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office, Surveillance Camera Code of Practice (2021)
- ICO – Guide to the UK GDPR
- ICO – Data protection and surveillance cameras (2021)
- ICO – Right of Access (Subject Access Requests) guidance
- DfE, Keeping Children Safe in Education (September 2025)

1.3. This policy operates in conjunction with the following school policies:

- Photography and Videos at School Policy
- Freedom of Information Policy
- Abuse Threats and Violence Policy GDPR Data Protection Policy.

2. Definitions

2.1. For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.
- CCTV - Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.
- The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school/ETB staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.
- Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).
- Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
- Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.
- Data Processing - performing any operation or set of operations on data, including: Obtaining, recording or keeping the data, Collecting, organising, storing, altering or adapting the data, Retrieving, consulting or using the data, Disclosing the data by transmitting, disseminating or otherwise making it available, Aligning, combining, blocking, erasing or destroying the data.
- Data Subject – an individual who is the subject of personal data.
- Data Controller - a person who (either alone or with others) controls the contents and use of personal data.
- Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an

organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

2.2. Hadley Learning Community does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

2.3. Any overt surveillance footage will be clearly signposted on entry onto the school site.

3. Roles and Responsibilites

3.1. The role of the data protection officer (DPO) includes:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes answers inferred from silence are non-compliant with the GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role. Monitoring the performance of the school's privacy impact assessment (PIA), and under the GDPR the data protection impact assessment (DPIA), and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.
- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

3.2. Hadley Learning Community, as the corporate body, is the data controller. The governing board of Hadley Learning Community therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The role of the Headteacher and Operations Manager include:

- Meeting with the Facilities Manager to decide where CCTV is needed to justify its means.
- Conferring with the DPO & Facilities Manager regarding the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

3.4. The role of the Facilities Manager

- Overall strategic design the CCTV system with consultation with the Headteacher, DPO, Operations Manager and IT Manager
- In line with the School Security policy make sure the school site is a safe and secure environment for all users
- Act as one of the day to day operators of the CCTV system, reviewing footage inline with the policy on behalf of the School.

4. Purpose and justification

4.1. The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.

4.2. Surveillance will be used as a deterrent for violent behaviour and damage to the school.

4.3. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

4.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.

5. The Data Protection Principles

- Data collected from surveillance and CCTV will be: Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Objectives

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

7. Protocols

7.1. The surveillance system will be registered with the ICO in line with data protection legislation.

7.2. The surveillance system is a closed digital system which does not record audio.

7.3. Warning signs have been placed on entry to the school site, as mandated by the ICO's Code of Practice.

7.4. The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

7.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

7.6. The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

8.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

8.2. The school's authorised CCTV system operators are:

Dylan Gilligan, Michael McElhone and Christine Arnold – Mitie, Facilities Management
Chris King - IT Manager
David Sotheran and Sam Hall, HLC ICT Technicians
Jack Whitehead – HLC Deputy Headteacher

8.3. The main control facility is kept secure and locked when not in use.

8.4. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

8.5. Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.

8.6. Surveillance and CCTV systems will not be intrusive.

8.7. CCTV can be viewed in the below places and using the web browsers on school machines to navigate to the NVR portals. Access to logging into the portals is managed and maintained by the IT Manager and Facilities Management.

- Reception (Showing external cameras and the gym)
- Facilities Managers Office (Site wide)

8.8. Any unnecessary footage captured will be securely deleted from the school system.

8.9. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

9. Privacy by design

9.1. The use of surveillance cameras and CCTV will be critically analysed using a PIA – under the GDPR this will become a DPIA but it will follow the same principles of a PIA.

9.2. A DPIA will be reviewed prior to the installation of any additional surveillance and CCTV system equipment.

9.3. If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

9.4. The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

9.5. If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek alternative provision.

10. Code of practice

10.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

10.2. The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based. +-

10.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.4. All surveillance footage will be kept for 31 days/one month for security purposes; the Headteachers and the Facilities Manager are responsible for keeping the records secure and allowing access.

10.5. The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

10.6. The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

10.7. The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

10.8. The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.

- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

10.9. Be accurate and well maintained to ensure information is up-to-date.

11. Access

11.1. Under the DPA 2018, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. All media containing images belong to, and remain the property of, the school.

11.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. The school will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Co-Headteachers, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one month of receipt.

11.11. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.12. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.13. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

11.14. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage 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.

11.15. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

11.16. Requests for access or disclosure will be recorded and the Headteachers will make the final decision as to whether recorded images may be released to persons other than the police.

11.17. Internal Access and requests to view footage should follow the protocols set out in Appendix 1

12. Monitoring and review

12.1. This policy will be monitored and reviewed on a biennial basis, or in light of any changes to relevant legislation by the DPO and the Headteachers.

12.2. The Headteachers will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

12.3. The Headteachers will communicate changes to this policy to all members of staff

13. Notification and Signage

The Headteacher will provide a copy of this CCTV Policy on request to staff, students, parents and visitors to the school. 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. Signage will also be prominently displayed at the entrance to Hadley Learning Community.

13. Appendix 1: Internal Access Protocols

1 Incident Occurs

- An incident on the school grounds occurs in which CCTV should be reviewed.

2 Request for Footage

- A Request for footage should be made to the ICT Team or Facilities manager via email and/or the online CCTV Access Request Form.
- Facilities Manager, SLT and SSMs do not require permission to request footage
- All other staff should get approval (via email) from the Facilities Manager / Headteachers / SLT for footage

3 Footage Reviewed

- ICT Team, Facilities Manager or Nominated Staff Member to review footage on behalf of requester
- ICT Team or Facilities Manager or Nominated Staff Memberto show footage to requester (If deemed appropriate)

4 Footage released or stored

- Footage can be released to SLT (Register of CCTV releases to be kept on behalf of DPO)
- Footage can be released to other staff members if approved by SLT/FM (release added to register)

5 Footage deleted

- Footage downloaded and stored on the Schools Secure SharePoint area is automatically deleted after 30 days. Once footage is deleted the CCTV release register should be updated on behalf of the DPO.

CCTV Data Release Request

Type of request	
	I would like to view CCTV footage.
	I would like to request a copy of CCTV footage.
	I would like to request the release of original CCTV footage.
NB we are not obliged to release footage that relates to another individual	

Your details			
Name			
Address			
Postcode			
Contact number			
Email			
ID provided	Driving Licence Passport Medical Card Birth Certificate Marriage Certificate Other		
Signature of Requestor		**Date:**	

Request details/incident	
Date of request	
Date of incident	
Time of incident	
Description of incident- *please provide as much detail as possible.*	
Reason for request	

All the details in this request form must be completed to ensure compliance with GDPR legislation and in line with guidance issued by the ICO			
Approved by	**(print)**	**Date:**	

13. Appendix 3: Internal Access Protocols

DATA SUBJECT ACCESS CCTV APPLICATION FORM

Under the terms of the Data Protection Act 2018 and UK GDPR, an individual is entitled to ask the school" / "Hadley Learning Community for a copy of all the personal information which it holds about him/her for the purposes of providing services to the individual. The information, which the individual is entitled to receive from the authority, includes a description of these purposes and the recipients to whom the data can be disclosed. This entitlement is known as the "Right of Access to Personal Data". Please complete this form, providing as much information as possible, should you wish to exercise your right in requesting disclosure of your data.

PLEASE NOTE THAT RECORDED DATA IS ONLY HELD FOR 30 DAYS BEFORE IT'S OVERWRITTEN. FOOTAGE WILL BE PROVIDED IN CCTV PROVIDED IN DVD ROM OR USB FORMAT. NO DATA WILL BE RELEASED THAT BREACHES CHILD PROTECTION POLICY.

1. Personal Details

Name:	
Address:	
Telephone Number:	

2. Information Required

Name:	
Address:	
Telephone Number:	

3. Declaration

I confirm that this is all of the personal data to which I am requesting access and which is held by the school for its purposes. I also confirm that I am the Data Subject and not someone acting on his/her behalf.

Signed: Date:

4. Fee & Proof of Identity

Under the Data Protection Act 2018 and UK GDPR, individuals have the right to access their personal data free of charge unless requests are manifestly excessive or repetitive.

We also require evidence that this enquiry is genuine. Therefore, please enclose copies of at least two proofs of identity, such as a driving licence, passport, recent utility bill etc.

Failure to provide these documents with your application will mean that your request is refused.

5. Postal Address

After completing the application form, please check to ensure that all the information you have provided is accurate and all required documents and the fee are enclosed.

Please return the application form to:

Operations Manager
Hadley Learning Community
Crescent Road
Hadley
Telford
TF1 5JU

Hadley Learning Community is committed to the principles defined in the Data Protection Act 2018 and Freedom of Information Act 2000. As such, information on this document will be used only for the purposes described above. We may, however, store the data in manual or electronic form, but only for as long as we are required to do so by law.

15. Appendix 3: Camera Locations

Camera Location	Area	NVR	Internal/External
AIMS room	Secondary	NVR3	Internal
AIMS room	Secondary	NVR3	Internal
AIMS room	Secondary	NVR3	Internal
AIMS shared area	Secondary	NVR2	Internal
AIMS shared area	Secondary	NVR3	Internal
AIMS shared area	Secondary	NVR3	Internal
Basketball court & pedestrian gate b	Secondary,Community	NVR3	External
Basketball court facing carpark c	Secondary	NVR3	External
Basketball court footpath facing school d	Secondary	NVR3	External
Bridge carpark crossing	Bridge	NVR2	External
Bridge carpark external	Bridge	NVR1	External
Bridge external primary entrance	Bridge	NVR1	External
Bridge F10 circulation	Bridge	NVR1	Internal
Bridge F10 Sec entrance	Bridge	NVR1	Internal
Bridge F11 entrance	Bridge	NVR1	Internal
Bridge F12 circulation	Bridge	NVR1	Internal
Bridge F12 primary entrance	Bridge	NVR2	Internal
Bridge lobby entrance	Bridge	NVR2	Internal
Camera 4 d	Primary	NVR3	External
Com - Basketball Court	Secondary,Community	NVR3	External
Com reception towards pool	Secondary,Community	NVR1	Internal
Comm fitness suite	Secondary,Community	NVR2	Internal
Comm fitness suite	Secondary,Community	NVR1	Internal
Comm Fitness suite	Secondary,Community	NVR3	Internal
Comm fitness suite entrance corridor	Secondary,Community	NVR2	Internal
Comm main entrance external	Secondary,Community	NVR1	External
Comm main entrance external	Secondary,Community	NVR3	External
Comm main entrance internal	Secondary,Community	NVR1	Internal
Comm main reception 360	Secondary,Community	NVR2	Internal
Comm pool change corridor	Secondary,Community	NVR1	Internal
Comm reception	Secondary,Community	NVR2	Internal
Comm ref change corridor	Secondary,Community	NVR1	Internal
Comm ref change external	Community	NVR2	External
Comm upper balcony	Secondary,Community	NVR1	Internal
Community upper black sofas	Secondary,Community	NVR1	Internal
ICT library	Secondary,Community	NVR1	Internal
Library lower	Secondary,Community	NVR1	Internal
Library upper	Secondary,Community	NVR1	Internal
Main access gates facing crossing b	Community	NVR1	External
Main access road c	Community	NVR1	External
Main access road facing crossing field c	Community	NVR1	External
Main access road facing gates a	Community	NVR1	External
Main access road facing MUGA d	Community	NVR1	External

Primary back stairs	Primary	NVR1	Internal
Primary carpark external b	Primary	NVR3	External
Primary carpark external c	Primary	NVR3	External
Primary entrance by fishbowl	Primary	NVR1	Internal
Primary external a	Primary	NVR3	External
Primary F1 back stairs	Primary	NVR1	External
Primary F1 circulation	Primary	NVR1	Internal
Primary F1 circulation	Primary	NVR1	Internal
Primary F1 external entrance	Primary	NVR2	External
Primary F1 side stairs	Primary	NVR2	Internal
Primary F2 corridor	Primary	NVR2	Internal
Primary F2 exit by hall into forum	Primary	NVR1	Internal
Primary F2 external playground	Primary	NVR2	External
Primary F2 EY corridor	Primary	NVR1	Internal
Primary nursery corridor	Primary	NVR1	Internal
Primary reception	Primary	NVR1	Internal
Sec area outside SSM offices 360	Secondary	NVR1	Internal
Sec carpark entrance access road b	Secondary	NVR1	External
Sec carpark facing deliveries d	Secondary	NVR1	External
Sec carpark facing entrance c	Secondary	NVR1	External
Sec carpark from access road a	Secondary	NVR1	External
Sec carpark from access road d	Secondary	NVR1	External
Sec dining	Secondary	NVR2	Internal
Sec dining	Secondary	NVR2	Internal
Sec dining	Secondary	NVR2	Internal
Sec dining	Secondary	NVR2	Internal
Sec F5 bottom stairs by sports hall	Secondary	NVR1	Internal
Sec F6 corridor	Secondary	NVR2	Internal
Sec F6 corridor far end	Secondary	NVR2	Internal
Sec F6 DT hub	Secondary	NVR2	Internal
Sec F6 engineering external	Secondary	NVR2	External
Sec F6 lower back stairs	Secondary	NVR2	Internal
Sec F6 pupil entrance	Secondary	NVR1	Internal
Sec F6 toilets lower	Secondary	NVR2	Internal
Sec F6 upper corridor	Secondary	NVR2	Internal
Sec F6 upper corridor	Secondary	NVR2	Internal
Sec F6 upper stairs	Secondary	NVR2	Internal
Sec F6 upper toilets	Secondary	NVR2	Internal
Sec F7 back stairs	Secondary	NVR2	Internal
Sec F7 corridor	Secondary	NVR2	Internal
Sec F7 corridor far end	Secondary	NVR2	Internal
Sec F7 staff entrance external	Secondary	NVR2	Internal
Sec F7 top of stairs	Secondary	NVR2	Internal
Sec F7 upper corridor	Secondary	NVR2	Internal
Sec F7 upper corridor	Secondary	NVR2	Internal
Sec F8 bottom back stairs	Secondary	NVR2	Internal

Sec F8 corridor	Secondary	NVR2	Internal
Sec F8 corridor	Secondary	NVR2	Internal
Sec F8 hub	Secondary	NVR2	Internal
Sec F8 stairs upper	Secondary	NVR2	Internal
Sec F8 upper corridor	Secondary	NVR2	Internal
Sec F8 upper corridor	Secondary	NVR2	Internal
Sec F8 upper corridor	Secondary	NVR2	Internal
Sec F8 upper corridor far end	Secondary	NVR2	Internal
Sec F9 back stairs	Secondary	NVR2	Internal
Sec F9 back stairs	Secondary	NVR1	Internal
Sec F9 carpark facing Bridge b	Secondary	NVR1	External
Sec F9 corridor	Secondary	NVR2	Internal
Sec F9 corridor far end	Secondary	NVR2	Internal
Sec F9 external facing Bridge a	Secondary	NVR1	External
Sec F9 toilet by deliveries	Secondary	NVR2	Internal
Sec F9 upper corridor	Secondary	NVR2	Internal
Sec F9 upper corridor	Secondary	NVR2	Internal
Sec F9 upper stairs	Secondary	NVR2	Internal
Sec F9 upper toilets	Secondary	NVR2	Internal
Sec F9 Delivery Entrance	Secondary	NVR 2	Internal
Sec music corridor	Secondary	NVR2	Internal
Sec PE staff base corridor	Secondary	NVR2	Internal
Sec pupil entrance external facing sports hall	Secondary	NVR2	Internal
Sec sport hall entrance by refs change	Secondary	NVR1	Internal
Sec sports hall corridor	Secondary	NVR1	Internal
Sec staff entrance internal	Secondary	NVR2	Internal

15. Privacy Impact Assessment (PIA)

Before a school/ETB installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. A school/ETB which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Act 2018. This is an important procedure to adopt as a contravention may result in action being taking against a school/ETB by the Office of the Data Protection Commissioner, or may expose a school/ETB to a claim for damages from a student.

Some of the points that might be included in a Privacy Impact Assessment are:

- What is the school/ETB's purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?
- Are the CCTV cameras intended to operate on the outside of the premises only?
- Is it justified under the circumstances?
- Is it proportionate to the problem it is designed to deal with?
- Is it intended that CCTV cameras will operate inside of the building?
- Are internal CCTV cameras justified under the circumstances?
- Are internal CCTV cameras proportionate to the problem they are designed to deal with?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the school/ETB need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Will the system being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Is the school/ETB, the data controller for the entire CCTV system (bearing in mind that some schools under the PPP are managed for operational purposes by management companies, in which case specific legal advice may need to be sought)?.
- Where a management company is in place, is the school/ETB satisfied that it complies with the Data Protection Acts with regard to the processing of images of staff, students and visitors to your school captured on any CCTV systems under its management?
- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, students and visitors been assured by the School that they will not be monitored and that the CCTV system will be used only for the stated purposes?
- Does the school's/ETB's policy on the use of CCTV make it clear that staff (teaching and non-teaching) will not be monitored for performance or conduct purposes?

- Have the views of staff & students regarding the location of cameras been taken into account?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been erected at the location of each internal camera indicating that recording is taking place and outlining the purpose of such recording?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images?
- Are those who will have authorised access to the system and recordings/images clear about their responsibilities?
- Are the camera monitors kept out of view of staff, students and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does the school have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (28 days) has expired?
- Does the school have a procedure in place for handling requests for access to recordings/images from a police authority?
- Will appropriate notices be in place to ensure that individuals know that they are being monitored?
- Does the school have a data protection policy? Has it been updated to take account of the introduction of a CCTV system?
- Does the school have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of forty days)?
- Has the right of access been communicated to staff, students and visitors?
- Has the school/ETB communicated its policy on the use of CCTV to staff, students and visitors and how has this been done?
- How are new students and new staff informed of the school's policy on the use of CCTV?