CCTV Policy & CCTV Data Protection Impact Assessment
Polisi CCTV ac Asesiad Effaith Diogelu Data CCTV

School / Ysgol:	Rhyl High School
Responsible / Cyfrifol:	Headteacher / Governing Body
Last Reviewed:	2 October 2025
Review Date:	2 October 2026

Cyngor sir ddinbych denbighshire County Council

"Being the best we can be"

"Be brave, risk being exceptional!

This Policy is a:

Please indicate (✓)

Statutory policy :
This is a model policy that has been developed by Denbighshire Education and Children's Services with schools and partners which school governing bodies can choose to adopt, or they must produce their own in line with the relevant guidance. ✓

Statutory policy :
This is a model policy that has been created without any formal consultation which school governing bodies can choose to adopt, or they must produce their own in line with the relevant guidance.

Non-statutory policy :
This is a model policy that has been developed by Denbighshire Education and Children's Services with schools and partners which school governing bodies can choose to adopt, or they must produce their own in line with the relevant guidance.

Non-statutory policy :
This is a model policy that has been created without any formal consultation which school governing bodies can choose to adopt, or they must produce their own in line with the relevant guidance.

This Policy relates to:

Please indicate (✓)

Rhyl High School (Secondary)	
All schools (please name)	
Other (please name)	

Headteachers Signature:

Mr P. Collins

Date: 2/10/25

Chair of Governors Signature:

Mr M. Harris

Date: 2/10/25

Cyngor
sir ddinbych
denbighshire
County Council

CCTV Policy & Procedure (Schools)

Table of Contents

1. Policy Statement

Rhyl High School uses CCTV surveillance systems within its premises. This policy provides information about the CCTV systems used and our position as to its management, operation and use.

The policy applies to all members of staff, pupils and visitors to Rhyl High School and any other persons whose images may be captured on the CCTV system.

CCTV is used for the purpose of providing a safe and secure environment and to protect school buildings and assets. CCTV operation is subject to the procedures set out in this policy and takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation ("GDPR")
- Data Protection Act 2018
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Surveillance Camera Code of Practice (issued by the UK Home Office)

'**CCTV**' refers to any type of camera used for the purpose of surveillance within this policy.

2. CCTV System Overview

a. The CCTV system is owned and managed by the school. The school is the 'data controller' for the images produced by the CCTV system and is registered with the Information Commissioner's Office. The Head Teacher is responsible for the overall management and operation of the CCTV system in accordance with the principles expressed in this policy.

b. CCTV operation is subject to a Data Protection Impact Assessment (DPIA) to assess the impact on individuals' privacy and ensure compliance with relevant legislation.

c. Signs shall be placed at main entrances to inform individuals that CCTV is in operation. The signage shall indicate who the system is managed by and includes a point of contact for further information. Signs shall also be erected where cameras are sited to inform individuals they are within an area in which CCTV is in operation.

d. The CCTV is in operation 24 hours a day, every day. Live images from CCTV cameras are streamed to a monitoring station within the school. Monitors shall be located in areas of restricted access.

e. The CCTV system, images and information shall be subject to appropriate security measures to safeguard against unauthorised access and use.

f. Business and Finance manager is appointed to act as Single Point of Contact for matters relating to the school's CCTV system. The Single Point of Contact shall also ensure that the school maintains appropriate records and documentation including:

- CCTV Policy & Procedures
- Data Protection Impact Assessment (DPIA)
- CCTV Asset list
- Record of persons authorised to access CCTV systems
- Cyber/Security measures in place to protect data
- Records of training undertaken by staff with access to or operating CCTV
- Annual review of CCTV use

The governing body may wish to receive an annual report of the system's performance and priorities including a brief overview of security checks and measures, compliments and complaints, disclosure requests etc.

g. Where the school is engaged in contract with a third party for the supply of CCTV operating services, the school shall ensure that relevant Security Industry Authority (SIA) licensing requirements are met. CCTV owned by the school, operated by its own staff and whose data is controlled by the school is classed as in-house and does not fall under SIA legislation.

3. Purpose

The school shall only use CCTV where it is necessary for specified and legitimate purposes:

- To provide a safe and secure environment for pupils, staff and visitors
- To protect school building and their assets
- To help prevent, detect and investigate crime

Footage may also be used as evidence during disciplinary, grievance and complaint

procedures.

4. Position of Cameras

a. Cameras shall be sited in such a way as to meet the purposes for which the CCTV is operated and shall be in prominent positions where they are clearly visible to pupils, staff and visitors. Areas in which CCTV is in operation are set out in Appendix 1.

b. Cameras shall usually be sited in communal areas such as corridors or entrances. Cameras shall not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance.

c. Where there is a heightened expectation of privacy, such as personal cellular offices, changing rooms or toilets, the school shall consult with the Data Protection Officer (DPO) with a view to consultation and completion of a specific Data Protection Impact Assessment (DPIA) in respect of siting cameras in these areas

d. Cameras capturing footage inside toilet cubicles or directed towards urinals shall not be permitted under this policy.

5. Monitoring & Access

a. Viewing of live CCTV images shall be restricted to authorised staff for the purposes stated in this policy.

b. Access to recorded images which are stored on the CCTV system shall be restricted to Site Manager/Senior Leadership Team for the purposes stated in this policy and for law enforcement purposes. Other school staff may view recorded footage on the direction of SLT.

c. Recorded images may be disclosed to Governors as part of an internal disciplinary proceeding, grievance procedure or complaint.

d. The school shall maintain a log all individuals accessing recorded CCTV images, including time and dates of access.

e. Unless an immediate response to events is required, staff should not direct cameras at an individual or a group of individuals.

f. Where covert surveillance is planned, authorisation must be sought and granted by an Authorising Officer of Denbighshire County Council in accordance with the Regulationof Investigatory Powers Act 2000 prior to commencement. If there is any doubt on the procedure guidance must be sought from the Council's Monitoring Officer/Head of Legal, HR and Democratic Services. Covert surveillance carried out by school staff without a form of authority from the Magistrates Courts may be subject to disciplinary action.

6. Storage & Retention

a. Any images recorded by the CCTV system shall be retained only for as long as is necessary for the purpose for which they were originally recorded.

b. Recorded images are stored for a period of up to 28 days unless there is a specific purpose for which they are retained for a longer period. Images shall be automatically or manually deleted after this period.

c. Where it is necessary for a specific purpose to retain images for a longer period, this shall be subject to regular review.

d. The school shall ensure appropriate security measures are in place to safeguard against unauthorised access to recorded images including:

- Restricting access to recording systems and retained images to authorised members of staff
- Restricting access to recording systems by appropriate security measures such as password protection
- The use of encryption for exported recordings.

7. Disclosure of images

a. Individuals captured on CCTV are 'data subjects' and can request access to CCTV

images of themselves.

b. Where an individual requests access to images of themselves, the request should be submitted on the standard form in Appendix 2. The school should respond within 1 month.

c. When such a request is made a specified staff member shall review the CCTV footage, in respect of relevant time periods and in accordance with the request.

d. If the footage contains only the individual making the request, then the individual maybe permitted to view the footage.

e. Where footage contains images of other individuals, advice should be sought from the Data Protection Officer and the school must consider:

- Whether the request *requires* the disclosure of others or can the images can be distorted so as not to identify them
- Whether the other individuals have consented to the disclosure of the images,
- Where consent is not sought or obtained, whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

f. A log must be kept of all disclosures.

8. Disclosure of Images to Third Parties

a. The school shall only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with this policy and the law. A record shall be kept of all such release of records.

b. Police and law enforcement agencies may request access to personal data including recorded images for the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment of collection of any tax or duty

c. The date, time, location, and incident for which CCTV recordings are requested should be specified on a Disclosure Request Form signed by an officer of the rank of inspector

or above.

d. The Data Protection Act does not give an automatic right of access to information. The school should assess the merit of each request received.

e. Should a record be required as evidence, a copy may be released to the police under the procedures described in this policy.

f. Records shall only be released to the police on the clear understanding that the record remains the property of the school, and both the record and information are to be treated in accordance with this policy.

g. The school also retains the right to refuse permission for the police to pass on the record or any part of the information contained therein to any other person unless a court order ordering disclosure is sought. The Police may require the school to retainthe stored records for possible use as evidence in the future.

h. If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advicemay be required.

9. Misuse of CCTV systems and recordings

CCTV images constitute personal data and appropriate data protection training shall be provided to staff who have access to live and recorded footage. The misuse of CCTV system and images could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.

10. Review of CCTV

The use of CCTV and the Data Protection Impact Assessment (DPIA) relating to it shall be regularly reviewed to ensure its operation remains necessary and proportionate in

meeting its stated purposes.

Complaints / Key Contact Points

Subject Access Requests for disclosure of CCTV images should be made by contacting rhyl.high@denbighshire.gov.uk

If you have a concern or complaint in relation to this policy or about the way we are collecting or using your personal data, you should raise your concern with the school or the Data Protection Officer for Schools in the first instance. Youcan also contact the Information Commissioner's Office

Key Contact details:

Schools Data Protection Officer
Lisa Jones, Legal Services Manager
Legal, HR and Democratic Services, Denbighshire County CouncilCounty Hall, Ruthin, Denbighshire. LL15 1YN
Tel: 01824 706275
dataprotection@denbighshire.gov.uk

Information Commissioner
Wycliffe
HouseWater
Lane
Wilmslow
Cheshire
SK9 5AF
Tel 03031231113
https://ico.org.uk

For further information about the Surveillance Camera Code of Practice:

Biometrics and Surveillance Camera Commissioner
scc@sccommissioner.gov.uk

The Commissioner has no powers to inspect or audit CCTV systems, or investigate any complaints

Appendix 1

CCTV locations

Camera	Area monitored
1	Outside and school entrances
2	Internal communal area's
3	
4	

UK Data Protection Act 2018 (General Data Protection Regulations – GDPR). RIGHT OF SUBJECT ACCESS APPLICATION FORM.

PLEASE NOTE THAT THIS FORM IS ALSO AVAILABLE IN WELSH.

Your Rights:

Under the terms of the UK Data Protection Act 2018 (GDPR) an individual has a right to access personal data which the School holds about him/her, subject to any exemptions that may apply.

Before information can be searched for and sent to you, your identity must be established. This is to ensure that not only do you receive the correct data but that other individuals cannot fraudulently obtain your data.

The UK Data Protection Act 2018 allows us one month in which to respond to your request. However, this period cannot start until we have all the information necessary to process the request.

This form is not obligatory but it would assist us if you would complete it and help us deal more quickly with your request.

If you would like to pursue your access rights, please answer the following questions:

SECTION 1 – Your Personal Details

This Section is for requesting your own personal information. Please complete Section 4 below if you are acting on another's behalf.

The information requested below is to help the School satisfy itself as to your identity and to find any data held about you. **Please use block capital letters**.

Title (Tick box if appropriate)	Mr		Mrs		Miss		Ms	
Other title (e.g. Dr, Rev, etc.)								
Surname/Family Name								
First Names								
Maiden/Former Names								
Sex (tick box)	Male		Female					
Date of Birth								
Email address								
Home Address								
Post Code				Tel No				

If you have lived at this address for less than two years, please also give your previous address:

Previous Home address	
Post Code	

Have you previously applied to the School for access to your personal data?

Yes ☐ No ☐

If so, please could you give the date of your application? .....

Proof of Identity

To help establish your identity, your application should be accompanied by copies of two of the following documents: -

Utilities Bill ☐

Driving Licence ☐

Passport ☐

Please do not send original documents, only copies, as these will not be returned.

SECTION 2 – The information you are requesting

If your request is for paper and electronic records and there is a specific item of personal information/data which you are seeking, please give the details below:

.....

.....

.....

.....

.....

.....

.....

.....

.....

If your request is for CCTV footage, please provide the following information:

Date	
Time	
Location	
Description of Incident, Vehicles and Person (s)	

SECTION 3 – Requesting another person's data

An application being made by someone acting on behalf of the data subject.

I confirm that I am acting on behalf of the data subject, namely ..... and I enclose herewith proof of my authority to act on behalf of the data subject (for example, a letter signed by the data subject authorising me, Power of Attorney, etc.).

Your relationship to the Data Subject		
Title (e.g. Mr)		
Surnames/Family Name		
First Name		
Home / Business address		
	Post Code	Tel No
Email address		

Proof of Identity

Proof of identity of agent to help establish your identity as the authorised agent. The application should be accompanied by copies of two of the following documents:

Utilities Bill ☐

Driving Licence ☐

Passport ☐

Evidence of parental responsibility (if applicable) ☐

Please do not send original documents, only copies.

SECTION 4 - Declaration

I request that you provide me with details of the personal data about me as I have indicated above.

I confirm that I am the data subject - I am asking for my own personal data.

OR

I confirm that I am acting on behalf of the data subject – I am asking for the personal data of someone else.

Signed ..... Date .....

Checklist

1 Have you filled in all of the parts of the application form relevant to your application?

2 Have you signed the form?

3 Have you enclosed identifying documents?

4 Where you are acting on behalf of the data subject have you enclosed proof of your authority to do so and completed Section 4?

Privacy Notice – what we will do with your details.

Your documents (the Subject Access Request form, the identifying documents, and any associated correspondence) will be processed by the School for the specific purposes of processing your Subject Access Request under the Data Protection Act 2018. The School will not share the data with any other organisation unless required by law. The School may need to share your data with the Information Commissioner' Office in the event of a complaint or with Denbighshire County Council under any service level agreements, as many Schools receive advice and support from the local authority.

The School will retain the documents for two years from the completion of the request.

If you feel that the School have mishandled your personal data at any time you can make a complaint to the Information Commissioners Office by visiting their website, or by calling their helpline on 0303 123 1113.

SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

Data protection impact assessments template for carrying out a data protection impact assessment on surveillance camera systems

Project name: CCTV

Data controller(s): Rhyl High School

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☒ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☒ Targeting children / vulnerable adults
☒ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

Personal data is processed in accordance with the UK GDPR and Data Protection Act 2018.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve? Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

Cameras are positioned to view communial areas within the school building, outside spaces/grounds / school entrances.

The system is required for the following overall operational reasons:
To provide a safe and secure environment for pupils, staff and visitors.
To protect school buildings and assets
To help prevent, detect and investigate crime

There have been increasing instances where pupils have been setting off the fire alarms and causing disruption to the school day – CCTV has acted as a deterrent and this has reduced
CCTV is also used to investigate incidents involving pupil safeguarding and behaviour

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

CCTV processes the personal data of pupils, staff and visitors within school premises.

Areas overlooked by cameras include external grounds, entrances, various communal areas and classrooms.
Camera locations are set out in Appendix One.

CCTV is operational 24 hours a day, 7 days a week.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

The Head / SLT will be responsible for making decisions about the uses of the system and who will have access to CCTV images.

Images may be shared in response to a request from law enforcement agencies e.g. Police, Courts and / or in response to Subject Access Requests by individuals or authorised third parties, in line with Data Protection Legislation.

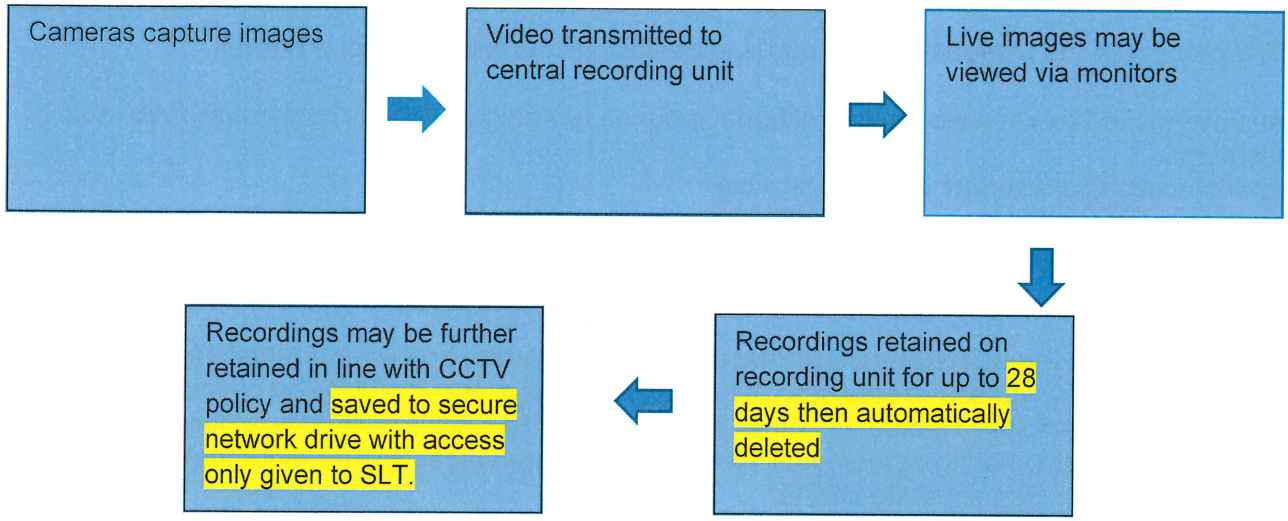
6. How is information collected? (tick multiple options if necessary)

- ☒ Fixed CCTV (networked)
- ☐ ANPR
- ☒ Stand-alone cameras
- ☐ Other (please specify)
- ☐ Body Worn Video
- ☐ Unmanned aerial systems (drones)
- ☐ Redeployable CCTV

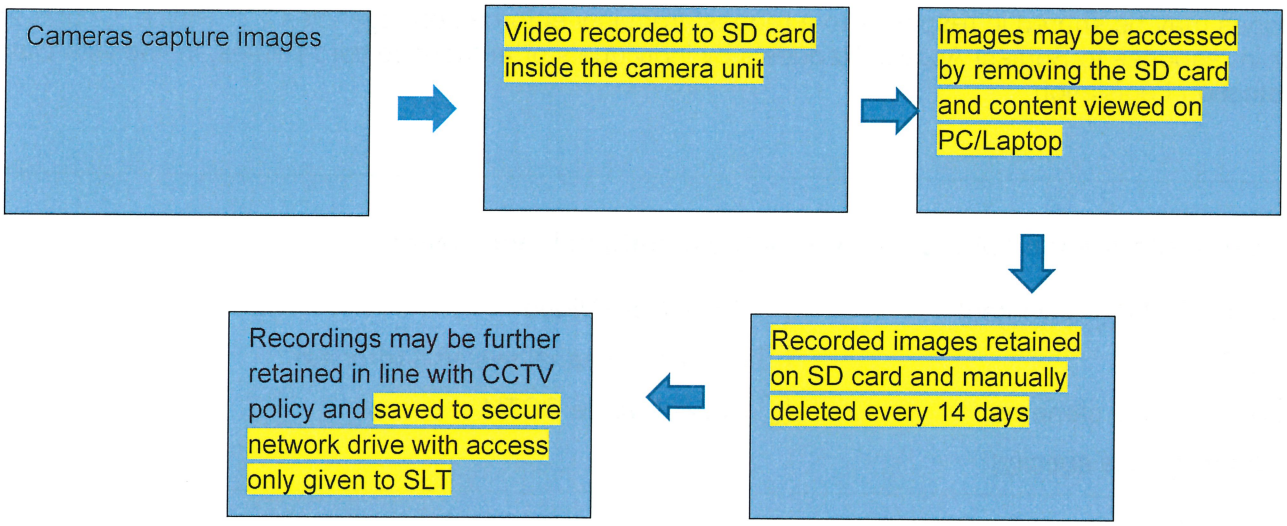
7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

Please check and amend as required

CCTV ADT



STAND ALONE CAMERAS



8. Does the system's technology enable recording?

☒ Yes ☐ No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

On-site

9. If data is being disclosed, how will this be done?

☒ Only by on-site visiting

☒ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)

☐ Off-site from remote server

☐ Other (please specify)

Where copies released, encryption will be used.

10. How is the information used? (tick multiple options if necessary)

☐ Monitored in real time to detect and respond to unlawful activities

☐ Monitored in real time to track suspicious persons/activity

☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.

☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☐ Linked to sensor technology

☐ Used to search for vulnerable persons

☐ Used to search for wanted persons

☒ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies

☐ Recorded data disclosed to authorised agencies to provide intelligence

☒ Other (please specify)

Footage may be used by the school to investigate incidents e.g.safeguarding / bullying / damage to property etc

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Schools DPO	Meeting		
Head Teacher	Meeting		
Governors	Written report to meeting of Governing Body		

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

The lawful basis we rely on for processing is legitimate interests.

It is within the legiimate interests of the school to ensure:
The safeguarding of pupils, staff and visitors
The protection of school buildings and assets

Behaviour incidents can cause disruption to the school day affecting the smooth running of the school and the ability of other pupils to learn e.g. setting off fire alarms

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

The School's CCTV Policy, including general areas monitored will be published in the school's website and a copy made available upon request.
The school's Information Asset Register will be updated to include processing via CCTV
Signs will be placed at main entrances to inform people that CCTV is in operation and will include a point of contact for further information. Signs will also be placed in the general area where cameras are sited.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

CCTV operation is subject to Data Protection Impact Assessments to consider necessity and proportionality. Necessity for CCTV will be reveiwed as appropriate.
DPO consulted
CCTV Policy & procedures will be reviewed at regular intervals.
Further DPIA's will be carried out where there is a change to use of CCTV.
Viewings of recorded images have to be approved by SLT.

15. How long is data stored? (please state and explain the retention period)

.
Footage is automatically retained on the central recording system up to 28 days and manually deleted from the SD card every 14 days.
There may times when there is a delay in reporting incidents such as bullying or damage to property therefore 4 weeks seems a reasonable time to retain the footage.

16. Retention Procedure

☒ Data automatically deleted after retention period

☒ System operator required to initiate deletion

☒ Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Under the GDPR, the school is required to ensure appropriate security measures are in place to prevent the unlawful disclosure of images. This will include:

- Access to recording systems and retained images is restricted to specified members of staff via locked door
- The CCTV system is password protected;
- Restriction of the ability to make copies to specified members of staff
- All exported recordings will be encrypted
- A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the school
- Cameras / system is regularly checked to ensure it is in correct working order

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

Right of Access - School has Data protection Policy including Subject Access Request procedure
Right to be informed - On-site signage
Right of erasure (in some circumstances) – School can consult with responsible person for Data Protection matters in the event of a request to delete a recording

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

All options were exhausted but due to the level of disruption to the school day with the fire alarm being set off continuously there was no other option.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

☐ The agencies that are granted access

☒ How information is disclosed

☒ How information is handled

Are these procedures made public? ☒ Yes ☐ No

Are there auditing mechanisms? ☐ Yes ☐ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

No internal audit as such but putting additional checking processes and usage of CCTV in place.

Identify the risks

I have completed this next section quite generally so far with a view to complete it after my visit to RHS

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Positioning of CCTV cameras and privacy concerns - use of CCTV could be unlawful if not necessary, proportionate and just	Possible	Significant	Medium
Security breach leading to loss, unauthorised disclosure or access to personal data – could lead to reputational damage and possible compensation claim/s	Possible	Significant	Medium
System use in breach of GDPR leading to enforcement action by the ICO / compensation claim/s	Possible	Significant	Medium
Non-compliance when upgrading the school's CCTV system – leading to enforcemet action by the ICO / compensation claim/s	Possible	Significant	Medium

Fault in system leading to data breach etc. leading to enforcemet action by the ICO / compensation claim/s	Possible	Significant	Medium

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved?**
Positioning of CCTV cameras and privacy concerns Cameras sited as far as possible in prominent areas, clearly visable, positioned towards open/communal spaces and to meet the overall purpose of CCTV operation. Appropriate CCTV signage in place to inform of cameras in operation Seek DPO advice and consider consultation and specific DPIA if cameras are considered in areas of heightened privacy expectation	Reduced	Low	Measure approved? Yes

Security breach leading to loss, unauthorised disclosure or access to personal data Ensure appropriate technical and organisational security measures in place Use access controls to system / cameras Access controls to offices / areas where system operated Only authorised access to footage stored / viewed	Eliminated reduced accepted		Measure approved?
System use in breach of GDPR Review use to CCTV to ensure use is adequate, relevant and no more than necessary for the stated purposes Data only retained as long as is necessary and viewed on request by SLT for a specific incident.	Eliminated reduced accepted		Measure approved?
Non-compliance when upgrading the school's CCTV system Consult with DPO when nature, scope or purpose of CCTV changes	Eliminated reduced accepted		Measure approved? Yes
Fault in system leading to data breach etc. Implement measures to check integrity / security of system and procedures	Eliminated reduced accepted	Low medium high	Measure approved? Yes

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. Further information is on the ICO website.

Item	Name/date	Notes
Measures approved by: Governing Body	Chair of Governors	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by: Headteacher	Mrs Claire Armitstead	If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:	Helen Roberts	DPO should advise on compliance and whether processing can proceed.
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments: Will continue to review the need for CCTV on annual basis		
This DPIA will be kept under review by: Olivia Beckett		The DPO should also review ongoing compliance with DPIA.

Date and version control: 19 May 2020 v.4

APPENDIX ONE

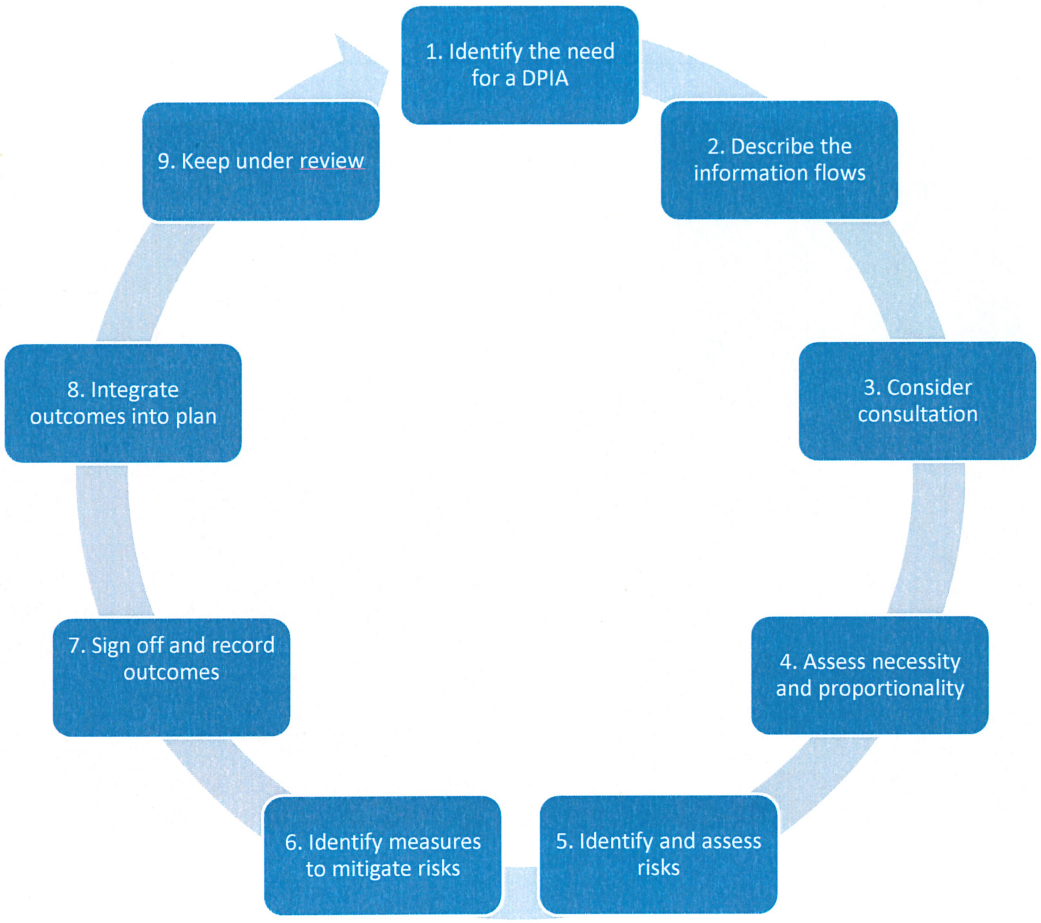
This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Please check and amend as required Updated 01/09/2025 The school currently has both 64 cameras within the school premises (external and internal) 63 cameras currently transmit video to a central recording unit, housed within the secure ICT server room. Monitors are located in the Caretaker's Office/ Main Reception/Behaviour intervention room. 1 stand alone camera currently record to an SD card situted inside the individual camera					
	CCTV		Images / audio		
External grounds	Dome / Fixed / Zoom	8	Images		Safeguarding / behaviour of pupils / protection of school buildings and assets
Entrances	Dome / Fixed / Zoom	4	Images		Safeguarding pupils
Internal communal areas	Dome / Fixed / Zoom	50	Images		Safeguarding / behaviour of pupils / protection of school buildings and assets
Classrooms	Dome / Fixed / Zoom	1	Images		Safeguarding / behaviour of pupils
	STAND-ALONE cameras				
Internal communal areas	Fixed	1	Images	By main exit door in reception	Safeguarding / behaviour of pupils / protection of school buildings and assets

Date and version control: 19 May 2020 v.4

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

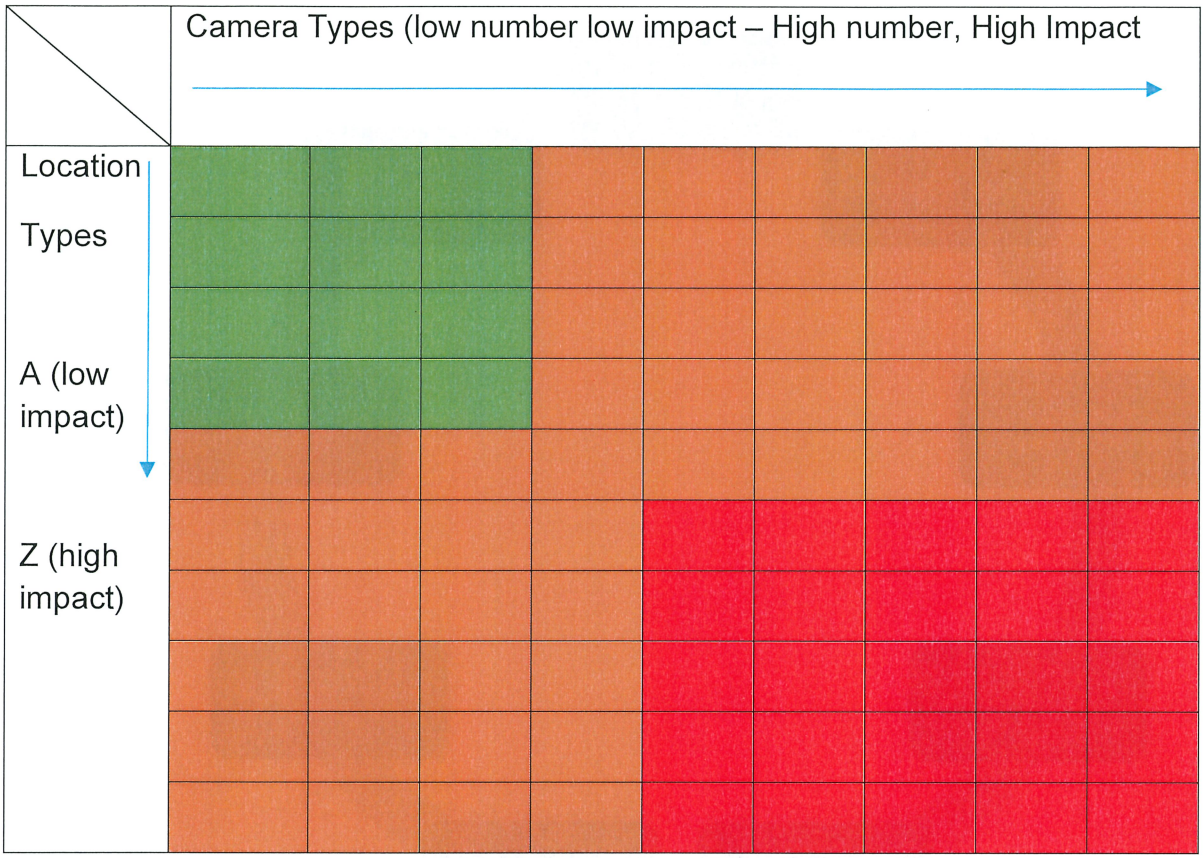


Date and version control: 19 May 2020 v.4

APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:



Date and version control: 19 May 2020 v.4

NOTES

Date and version control: 19 May 2020 v.4