



**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: Installation of CCTV system for school safety and security

Data controller(s): Holly Hill Church School, Mark Carr - Head Teacher

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 DPIA¹:

- | | |
|---|--|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data |
| <input checked="" type="checkbox"/> Public monitoring | <input type="checkbox"/> Innovative technology |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Data matching | <input type="checkbox"/> Invisible processing |
| <input type="checkbox"/> Tracking | <input checked="" type="checkbox"/> Targeting children / vulnerable adults |
| <input checked="" type="checkbox"/> Risk of harm | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input checked="" type="checkbox"/> Other (please specify) |

Safeguarding obligations within an educational setting

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)?

New system installed in 2025 to replace previous out-dated system. Processing is carried out under UK GDPR and Data Protection Act 2018. System is fully operational.

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.

- CCTV is installed across the school site to:
- Safeguard pupils, staff, and visitors
 - Prevent unauthorised access and trespassing
 - Deter vandalism and anti-social behaviour
 - Support investigation of incidents and complaints

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?

Data subjects:

- Pupils (children)
- Staff
- Parents/guardians
- Visitors and contractors

Data collected:

- Video footage
- Time/date stamps

Coverage:

- Entrances and exits
- Perimeter gates and fencing
- Playground areas
- Corridors and shared spaces

Not covered:

- Toilets, changing rooms, or private areas

Processing is continuous

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.

Authorised users:

- Headteacher
- Bursar
- IT Company (SCG/TelGroup) technical access only)

Data may be shared with:

- Police (crime investigation)
- Local Authority (safeguarding)
- Insurance providers (where necessary)

All sharing is:

- Recorded
- Lawful
- Case-by-case

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.

- Cameras capture video footage
- Footage transmitted via secure internal network
- Stored on on-site secure server (NVR system)
- No live monitoring except when required
- No facial recognition or biometric processing
- No watchlists used
- Footage automatically deleted after retention period

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.

- Recording is undertaken:

 - On-site (school-based recording system)
 - No audio recording enabled

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)

Method:

- Encrypted digital files
- Secure transfer or password-protected media
- Logged and authorised release only

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)

Other:

- Internal investigation of safeguarding or behavioural incidents or to monitor site security

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 |
|------------------------------|----------------------------|---------------------------|----------------------------|
| School staff | Staff meetings | Concerns about monitoring | CCTV policy and access log |
| Parents | Notices around school | | Policies updated |
| Pupils (indirect) | School communication | Awareness | Clear signage installed |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

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.

- Article 6(1)(e) – Public task (education and safeguarding duties)
 - Article 6(1)(f) – Legitimate interests (security)
- No intentional processing of special category data.

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.

- CCTV signage displayed throughout school
 - CCTV Policy updated
 - Additional information available on request
- Individuals would reasonably expect CCTV in a school for safeguarding

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?

- Cameras positioned to minimise intrusion
 - No coverage of sensitive/private areas
 - Footage accessed only when necessary
- Effectiveness monitored through:
- Incident reduction
 - Safeguarding outcomes

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

Footage retained for 30 days, unless required for investigation

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)

Exception: Footage retained longer if required for safeguarding or legal purposes

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?

- Password-protected system
 - Restricted access (authorised staff only)
 - Access logs maintained
 - Secure internal network
 - Staff training on data protection
 - Supplier contract includes GDPR compliance
- No international data transfers.

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.

- Subject Access Requests handled within 1 month
- Identity verification required
- Third-party data redacted where necessary
- Complaints handled via school complaints process

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.

- Improved lighting
 - Increased staff supervision
 - Physical security measures
- These were insufficient alone; CCTV provides additional safeguarding assurance.

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)

Access logs, data disclosures, annual review of policies

Identify the risks

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 | Severity of harm | Overall risk |
|---|--|---|-------------------------------|
| Excessive monitoring of children | Remote, possible or probable Possible | Minimal, significant or severe Significant | Low, medium or high Medium |
| Unauthorised access to footage | Possiblr | Significant | Medium |
| Misuse of footage | Remote | Significant | Medium |
| | | | |

| Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. | Likelihood of harm | Severity of harm | Overall risk |
|---|------------------------------|--------------------------------|---------------------|
| | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |
| | | | |
| | | | |
| | | | |
| | | | |

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 | Residual risk | Measure approved? |
| Restricted access controls | Eliminated reduced accepted Reduced | Low medium high Low | Yes/no Yes |
| Staff training | Reduced | Low | Yes |
| Clear policy & purpose limitation | Reduced | Low | Yes |

| Options to reduce or eliminate risk | Effect on risk | Residual risk | Measure approved? |
|-------------------------------------|---|------------------------|-------------------|
| Limited retention purpose | Eliminated reduced accepted Reduced | Low medium high Low | Yes/no Yes |
| Signage and transparency | Reduced | Low | 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: Head Teacher | Mark Carr 23 rd April 2026 | Integrate actions back into project plan, with date and responsibility for completion. |
| Residual risks approved by: Head Teacher | Mark Carr 23 rd April 2026 | 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: Jackie Ingleby | 23 rd April 2026 | DPO should advise on compliance and whether processing can proceed. |
| Summary of DPO advice Processing is proportionate and compliant with UK GDPR provided safeguards are maintained. | | |
| DPO advice accepted or overruled by: Head Teacher (specify role/title) | Mark Carr 23 rd April 2026 | If overruled, you must explain your reasons. |
| Comments: Accepted | | |
| Consultation responses reviewed by: | | If your decision departs from individuals' views, you must explain your reasons. |
| Comments: | | |

Date and version control: 19 May 2020 v.4

| | | |
|---|--|--|
| This DPIA will be kept under review by: | | The DPO should also review ongoing compliance with DPIA. |
|---|--|--|

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) |
|-------------------|-------------------|--------|-----------|------------|--|
| School entrances | Fixed CCTV | 4 | 24hrs | Limited | High safeguarding need |
| Playgrounds | Fixed CCTV | 9 | 24hrs | Limited | Protects pupils |
| Blossom Classroom | Fixed CCTV | 1 | 24hrs | Limited | Protects pupils and staff, gih safeguarding need |
| Perimeter | Fixed CCTV | 7 | 24hrs | Limited | Site Security and safeguarding |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



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:

| | Camera Types (low number low impact – High number, High Impact) | | | | | | | | |
|-----------------|---|--------|--------|--------|--------|--------|--------|--------|--------|
| | → | | | | | | | | |
| Location | Green | Green | Green | Orange | Orange | Orange | Orange | Orange | Orange |
| Types | Green | Green | Green | Orange | Orange | Orange | Orange | Orange | Orange |
| A (low impact) | Green | Green | Green | Orange | Orange | Orange | Orange | Orange | Orange |
| Z (high impact) | Orange | Orange | Orange | Orange | Red | Red | Red | Red | Red |
| | Orange | Orange | Orange | Orange | Red | Red | Red | Red | Red |
| | Orange | Orange | Orange | Orange | Red | Red | Red | Red | Red |
| | Orange | Orange | Orange | Orange | Red | Red | Red | Red | Red |
| | Orange | Orange | Orange | Orange | Red | Red | Red | Red | Red |

NOTES

Date and version control: 19 May 2020 v.4

