**DATA PROTECTION IMPACT ASSESSMENT for CCTV [Name of School]**

Contents

[Data Protection Impact Assessment - CCTV 3](#_Toc130286098)

[Details of Assessment 3](#_Toc130286099)

[Reason for DPIA 3](#_Toc130286100)

[The System 4](#_Toc130286101)

[Processing 4](#_Toc130286102)

[Consultation 7](#_Toc130286103)

[Necessity and Proportionality 8](#_Toc130286104)

[Risks 11](#_Toc130286105)

[Mitigating Risks 12](#_Toc130286106)

[Authorisation 13](#_Toc130286107)

[Appendix One - CCTV Setup 15](#_Toc130286108)

**\*\*\*Using this Template\*\*\***

**Guidance**

This template is for schools / trusts completing a Data Protection Impact Assessment (DPIA) for CCTV. A DPIA will assist in assessing and mitigating any privacy issues linked to the use of a surveillance system.

The guidance ‘Data Protection Impact Assessment for CCTV - Carrying Out A Data Protection Impact Assessment On Surveillance Camera Systems’ should be read before completing the template.

A DPIA CCTV should be completed when:

* CCTV is being considered.
* New technology or functionality is being added on to an existing system
* There are plans to process more sensitive data
* Images will be captured from a different location

The following are key considerations when developing your DPIA:

* Do you have a lawful basis for any surveillance activity?
* Is the surveillance activity necessary to address a pressing need, such as public safety or the prevention, investigation, detection or prosecution of criminal offences?
* Is surveillance proportionate to the problem that it is designed to mitigate?
* The governance and accountability arrangements for any surveillance camera system and the data it processes musts also be considered.

If the answer to any of the first three questions is ‘**no**’, then use of surveillance cameras in your school is not appropriate.

You may have to consult your IT Department or CCTV provider, as well as your DPO, while completing this DPIA. Where risk identified cannot be mitigated you may have to contact the ICO. Risks should be recorded in your school’s/academy’s risk register.

A DPIA is not a one-off exercise. Your DPIA CCTV should be reviewed at least annually and updated either when you are considering a technical refresh/upgrade or when you are considering introducing new technology or functionality to your CCTV system. Details of that annual review should be recorded in the Authorisation section of this template.

**Instructions**

***Please read the guidance before attempting to complete the DPIA.***

Where you see square brackets ‘[ ]’ your approach regarding this point needs to be considered before making any changes.

* Importantly, answer all questions
* You may have to speak with the IT department, if in-house, or your contractor, to identify the technical aspects of the proposed CCTV/modifications.
* If you are unsure of the questions being asked contact One West for advice.
* When all points have been considered you should discuss the DPIA, and any risks identified with the DPO and then your Trustees/Board of Governors .
* Once all changes have been made, delete the square brackets and their contents.

Where you see highlighted text replace with the appropriate/preferred name and details.

Finally, *delete* this text box and save the file to your set of data protection related documents. *Note the importance of recording the completion of this DPIA in your school’s document control system*.

Guidance covering completion of DPIA for CCTV provided by One West may help completing this DPIA. The DPIA 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.

# Data Protection Impact Assessment - CCTV

## Details of Assessment

### School name:

### Data controller(s):

### Date DPIA completed:

**DPIA Control Record**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Reason for DPIA

### 1. Identify why your deployment of surveillance cameras requires a DPIA

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)?

|  |
| --- |
|  |

## The System

### 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 period; housing and community issues, etc.

|  |
| --- |
| The school / All schools within the Trust may use CCTV in various locations across the Trust to ensure the safety and security of the sites and of all users of the sites. Monitoring may allow staff to identify and deter incidents where staff may not be present. Footage will also assist in any post incident evaluation. Where necessary cameras may be used for the prevention and detection of crime and anti-social behaviour and for the protection of school property. For example through deterring vandalism, bullying and discouraging anti-social behaviour including alchol and drug related issues. Footage may also be used or shared with law enforcement bodies where necessary for the apprehension and prosecution of offenders.  CCTV helps protect school property and provides an additional layer of assurance regarding the safety of pupils, staff and visitors through deterring potential incidents. It may support the police in a bid to deter and detect crime and in identifying, apprehending and prosecuting offenders.  The Trust and its academies will adhere to the ICO’s code of practice for the use of CCTV. The Trust does not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras, where in use, will be clearly visible and accompanied by prominent signs explaining that CCTV is being used. |

### 4. 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.

|  |
| --- |
| A number of measures are already in place to provide safety for staff and pupils. However the use of CCTV will provide support to existing practices and it will only be used where there there is considered to be a higher level of risk.  The system is operational 24/7 in locations where it has been deemed necessary. |

## Processing

### 5. 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 will be those people, including staff, parents/carers, children and visitors and local residents who cross the field of view of the CCTV during the periods it operates. The populations may include pupils and members of staff and visitors to the school. The population is approximateley ‘n’ pupils/staff and ‘n’ visitors per day. Data and information gathered by the CCTV will be retained for the period defined in the school/academy’s RoPA and Retention Schedule. At the end of that period data and information will be disposed of appropriately. |

### 6. 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 images will be used by the school and may be shared with the police where necessary and lawful for the investigation of crime and antisocial behaviour and evidential purposes.  The Data Controller is the Headteacher (name) who will retain ultimate control of the information and decisions around how it can be used. This includes how long the data is retained and how it is disposed of. If for any genuine law enforcement purpose, it becomes necessary to pass footage to the Police then they will assume responsibility (be Data Controller) and data will be processed in line with the Law Enforcement Provisions of the DPA 2018 under Part 3 Section 31. |

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

Fixed CCTV (networked)  Fixed CCTV (Not networked)  Body Worn Video

ANPR  Unmanned aerial systems (drones)

Stand-alone cameras  Re-deployable CCTV  Other (please specify)

|  |
| --- |
|  |

### 8. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram.

Indicate whether the information 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.

|  |
| --- |
| Use/interaction with CCTV is limited to ‘checking/using it’ during day-time operations and only referring to recording if there is suspicison of something untoward. |

### 9. Does the system’s technology enable recording?

Yes, specify location below.  No

If recording is enabled, state where it is undertaken (no need to stipulate address but may include local authority CCTV Control room or a third-party contractor’s control room, if your system is connected to one, on-site, if the system and recordings stay at school and on site will suffice for stand-alone camera or body worn video). Also note whether the surveillance equipment enables audio recording.

|  |
| --- |
| Images will be recorded and stored on stand-alone machine located in a locked front office in the school with strict access controls/permissions. Hence only specified individuals will have access to the CCTV recording system. The images are not backed up on existing school wide networks. No third-party organisation will be involved in monitoring or storing images. |

### 10. 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)

|  |
| --- |
| Data will not be disclosed routinely. Data will be stored for up to 31 days or longer if it forms the basis of an investigation. Disclosure will only be provided either in response to a subject access request (SAR), which should follow the process defined at the School’s / Trust’s SAR process, or following a request made by law enforcement agencies, such as the police. |

### 11. 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)

|  |
| --- |
| Real time monitoring is limited to the hours that the school is in operation. Recorded images taken outside the school’s normal operating hours may be reviewed at the next opportunity but are only likely to be looked at when there is suspicion that an incident has occurred. |

## Consultation

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

Please outline the main comments from the ‘public’ resulting from your consultation: as part of a DPIA.

|  |  |  |  |
| --- | --- | --- | --- |
| Stakeholder consulted | Consultation method | Views raised | Measures taken |
| Staff |  |  |  |
| Parents/Carers |  |  |  |
| Local Residents |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Necessity and Proportionality

### 13. 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.

|  |
| --- |
| **Important Note**  Under Health and Safety legislation, schools are responsible for day-to-day health and safety whenever pupils are in the care of school staff - this includes school trips and clubs.  Under the Health and Safety at Work Act 1974 and The Management of Health and Safety at Work Regulations 1999, employers have a responsibility to assess and avoid or reduce risks, particularly around lone workers as potential dangers facing them can be different or more acute.  Relevant and sufficient security measures and procedures help (school name) to comply with relevant regulations by helping to protect pupil and staff from violence, bullying and aggression as well as deterring crime.  The following lawful bases apply to the processing of personal data captured by school CCTV systems:   * GDPR Article 6 (1)(c): Compliance with a legal obligation including Management of Health and Safety at Work Regulations 1999, Health and Safety at Work Act 1974, Crime & Disorder Act 1998 * GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in (school name) i.e. keeping our pupils safe at school. * GDPR Article 6 (1)(f): Where (school name) is processing CCTV footage for a legitimate reason other than performing its tasks as a public authority then this processing may be necessary for the purposes of our (or someone else's legitimate interests), except where overridden by the data subject’s data protection rights and freedoms. The school and its visitors have a legitimate interest in being in a safe and secure environment while the legitimate interests of the school include protecting school buildings and property and the prevention and detection of crime and staff and visitor safety.   Where processing personal data involves special category data (as defined by the GDPR) then (school name) will ensure that one of the special category conditions apply as per Article 9 of the GDPR and that this is recorded. This is likely to be (but not limited to):   * Article 9 (2) (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.   In line with the Data Protection Act 2018 Schedule 1 Part 2, one or more specific ‘substantial public interest’ conditions for Article 9(2)(g) will apply. This may be, but is not limited to:  DPA 2018 Schedule 1, Part 2, Para 6: Statutory etc and government purposes  DPA 2018 Schedule 1, Part 2, Para 10: Preventing or detecting unlawful acts  DPA 2018 Schedule 1, Part 2, Para 18: Safeguarding of children and of individuals at risk |

### 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?

|  |
| --- |
| The CCTV comprises a number (n) cameras with fixed positions that give restricted fields of view and a number (n) cameras that can be panned, tilted and zoomed to focus on an area of interest. The position of cameras cannot be changed without considering the potential impacts on data subjects, which would lead to a review and update of this DPIA. |

### 15. 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.

|  |
| --- |
| Signage that declares an area is under surveillance will be positioned on the edge of an area. Privacy notices for parents/carers, the school’s workforce and visitors will advise parties of the use of CTTV at (school name). Periodically, parents and carers and staff will be reminded of the use of CCTV in school newsletters / staff bulletins. |

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

|  |
| --- |
| X days. |

### 17. 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)

Is retention of data and information recorded in the retention schedule.

|  |
| --- |
| The data is ‘automatically’ over written after 31 days but there is the facility to override the function to protect data that may be required by either a prosecution / law enforcedment agency or any other body that has responsibility for safeguarding of pupils.  Summarise process here. |

### 18. 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?

|  |
| --- |
| The CCTV runs automatically. An operator will only refer the school’s CCTV to monitor a developing situation (during day-time hours) and recordings will only be reviewed should an incident/potential incident/potential offence be suspected. Access to the CCTV system is limited to specified personnel at the school. The recording system is not connected to the existing school-wide networks and has no connection to the internet. |

### 19. 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.

|  |
| --- |
| Summary taken the SAR process may be added here. |

### 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 the policy/policies and by whom and when disclosure and information handling, such as disclosure, production, accessed, handled, received, stored information, is audited.

|  |
| --- |
| The School name / Trusts name CCTV Policy provides details of the processes underpinning operation of the CCTV system and recording system at the school. The operation of the CCTV system and the related recording system will be reviewed and audited annually as part of the annual review of this DPIA. |

## Risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to your camera system. Consider how long will recordings be retained? Will they be shared? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Assess both the likelihood of a risk occurring and the severity of any impact on individuals.

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 high Impact) | | | | | |
| Location  A (low impact)  Z (high impact) |  |  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |
|  |  |  |  |  |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk Id | 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) |
|  | Keen to understand the location of the CCTV internally |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*Add more rows if needed.*

## Mitigating 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. Assess residual levels of risk.

Note that Appendix One allows you to record mitigations and safeguards particular to specific camera locations and functionality.

| Measures to reduce or eliminate risks identified as medium or high risk | Risk Id | Effect on risk  (Eliminated, reduced, accepted) | Residual risk  (Low, medium, high) | Measure approved?  (Yes/no) |
| --- | --- | --- | --- | --- |
| Confirmation of the position of CCTV cameras to avoid overlooking neighbouring properties/residential |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*Add more rows if needed.*

## 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.

### Measures approved by:

Integrate actions back into project plan, with date and responsibility for completion

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

### Residual risks approved by:

If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

### DPO advice provided:

DPO should advise on compliance and whether processing can proceed

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| DPO | One West, Lewis House, Manvers Street, Bath, BA1 1JG |

|  |  |
| --- | --- |
| Date |  |

|  |  |
| --- | --- |
| Summary of DPO advice |  |

### DPO advice accepted or overruled by:

If overruled, you must explain your reasons.

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

|  |  |
| --- | --- |
| Comments |  |

### Consultation responses reviewed by:

If your decision departs from individuals’ views, you must explain your reasons

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

|  |  |
| --- | --- |
| Comments |  |

### This DPIA will kept under review by:

The DPO should also review ongoing compliance with DPIA

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

### DPIA Reviews

**Year One:**

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

**Year Two:**

|  |  |
| --- | --- |
| Name |  |

|  |  |
| --- | --- |
| Date |  |

## Appendix One - CCTV Setup

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 type | Camera types used | Number | Recording | Monitoring | Assessment of use of equipment (mitigations or justifications) |
| School entrance | All | 3 | 24hrs | 24hrs (only maximum 3 operators). | The privacy level expectation in school entrance likely to be high. School entrance well signed with appropriate signage for CCTV its use and purpose with contact details. |
| Classrooms | 1, 2, 5 | 12 (one per classroom) | When school is occupied | When school is occupied |  |
| Corridors | 1, 5 | 4 | When school is occupied | When school is occupied | HD camera only include due to proximity to town HD cam |
| Play areas | 4 | 6 |  | When school is occupied | Children safety on equipment |
| School buildings | 4 | 6 | 24hrs (calendar month) |  | High level anti-social behaviour - historical problems (please see statistical assessment in annual review). The privacy level expectation around school buildings likely to be low, although school well signed with appropriate signage for CCTV its use and purpose, with contact details. |

Notes:

1. Location type: List and categorise the different areas covered by surveillance on the system. Examples are provided above.
2. Camera types use: details from asset register that should describe equipment installed (type and number). Cameras may be categorised: ‘fixed wide-angle’, ‘remote control, no zoom’, ‘remote control, with zoom’ and ‘remote control, with zoom and two-way audio’.