

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

Project name: Summerhill School CCTV

Data controller(s): Summerhill School and Mitie

---

---



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<sup>1</sup>:

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

There is an existing surveillance camera system that covers external areas, school and sport reception areas. This will continue to be managed externally by Mitie.

The new deployment of a surveillance camera system will be internal covering corridors and stairwells. This will be managed internally by Summerhill School.

The data will be processed under the UK Data Protection Act 2018 and UK GDPR

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.

A Data Protection Impact Assessment is recommended by the Surveillance Camera Code of Practice which sets out the guiding principles that should be applied when CCTV systems are in place to ensure that privacy risks are minimised whilst ensuring the aims of the CCTV system are met.

<sup>1</sup> <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/>

CCTV consistently delivers benefits in terms of improved safety and security within schools.

It complements other security measures which are in place within the school such as external lighting.

The CCTV at Summerhill School aims to achieve the following:

- Improve the safety and security of students, staff, and visitors
- Protect the school buildings and internal infrastructure
- Improve student behaviour
- Encourage students to be prompt at the start of the lesson - Reduce vandalism
- Provide assistance in the detection and prevention of crime

Parents will have the assurance that their children are safe whilst in school. Parents are aware that with CCTV there is the potential for behaviour at school to improve. The Board of Governors are also of the opinion that this is the case

The CCTV system will be used to ensure the safety and security of students, staff and visitors. They data will be used to detect unauthorised visitors, students with poor behaviour/internal truancy, and protect school assets from damage. The information may be shared with the Senior Leadership Team and the Police for investigation and enforcement purposes.

Disclosure of data is covered by the school's internal processes which are fully compliant with relevant legislation and Codes of Practice.

Statistics to support this in terms of vandalism, issues around behaviour. Has there been an upward trend since CCTV has been unavailable?

This compares with £12,008 for the financial year April 2020 to March 2021. Costs incurred since April 2021 has been £2,333 for acts of vandalism.

These figures do not take into account the resources employed in investigating and followup work.

**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?

The internal CCTV Surveillance System will provide the school with video pictures from 21 fixed-base cameras located throughout the school in corridors and stairwells. The images will be captured on a digital video recorder located within the school. The CCTV system will be operational 24 hours a day, 7 days a week.

The 21 additional cameras will be located in areas where students and staff have access. Cameras will not be located in sensitive areas where privacy is expected: there will be no cameras in toilets or changing rooms. Some cameras will be located in the corridors outside toilets and changing rooms - these cameras will be positioned so that they cannot observe any area where privacy is expected.

Data captured will include images of students, staff, and visitors to the school including contractors and other professionals, etc.

By default the CCTV may be picking up special category data including race/ethnic origin and the health of an individual but this is not the purpose of the system.

The internal CCTV Surveillance System will capture video images, which are transmitted from cameras positioned in various locations throughout the school. All of the internal CCTV cameras will be fixed on a particular scene. The location of the cameras will be:

- 5 fixed cameras on Ground Floor
- 9 fixed cameras on First Floor
- 7 fixed cameras on Second Floor

The images will be captured to a Digital Video Recorder which will be housed within a secure area. Access to the room will be restricted. The images will be stored on the hard drive of the Digital Video Recorder.

Designated members of the Senior Leadership Team will have access to the CCTV images. This will help to maintain site security, access control, student and staff safety.

Images will be retained for 30 days unless requested as part of an incident and then stored on archive for 12 months. The Data Management System will automatically delete the information after 30 days. Please see the school's Data Retention Policy.

The external CCTV Surveillance System will continue to be managed by Mitie as data controller.

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 external CCTV Surveillance System will continue to be managed by Mitie as data controller.

The internal CCTV Surveillance System will be managed by Summerhill School as data controller.

The school has a CCTV Policy. The system will be operated in line with relevant legislation and the Surveillance Camera Code of Practice. Staff operating/using the system will have undertaken Data Protection and Information Security training.

Summerhill School's use of the CCTV Surveillance System will respect the rights of access to personal data under UK Data Protection Law.

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

- |   |                                     |
|---|-------------------------------------|
| <input checked="" type="checkbox"/> Fixed CCTV (networked) Body | <input type="checkbox"/> Worn Video |
| <input type="checkbox"/> ANPR Unmanned aerial systems           | <input type="checkbox"/> (drones)   |
| <input type="checkbox"/> Stand-alone cameras Redeployable       | <input type="checkbox"/> CCTV       |
| <input type="checkbox"/> Other (please specify)                 |                                     |

The fixed CCTV camera does not have PTZ (pan, tilt, zoom) facility.

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.

The CCTV system will provide the school with video images from 21 fixed-base cameras located throughout the school. Images will be transferred to the video recorder by fixed network cabling. The CCTV system will be operational 24 hours a day, 7 days a week.

The CCTV images will be obtained within the confines of the school building including corridors and stairwells. Cameras will be located in areas where students and staff have access. All of the CCTV Cameras will be fixed on a particular scene. The location of the CCTV cameras will be as follows: 5 fixed cameras on Ground Floor

9 fixed cameras on First Floor

7 fixed cameras on Second Floor

The cameras will not capture audio.

There will be no use of integrated surveillance technologies such as automatic facial recognition.

The images will be captured to a Digital Video Recorder which will be housed within a secure room. Access to the room will be restricted. The images will be stored on the hard drive of the Digital Video Recorder.

The captured images may be viewed live by designated persons (eg nominated members of the Senior Leadership Team). This will help to maintain site security, access control, student and staff safety.

Images will be retained for 30 days unless requested as part of an incident and then stored on archive for 12 months. The Data Management System will automatically delete the information after 30 days. Please see the school's Data Retention Policy.

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.

The images will be captured to a Digital Video Recorder which will be housed within a secure room. Access to the room will be restricted. The images will be stored on the hard drive of the Digital Video Recorder.

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)

Copies of footage may be released as part of a subject access request or where the lawful basis is clearly identified.

Where requests are made to access CCTV footage the school will have a CCTV access log to record date of the request, who by, information provided, purpose, provided to third party, data securely sent, copy retained and its location.

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)

The system will not routinely be monitored in real time but this may take place if this is required.

Data may be disclosed to authorised agencies, i.e. local authority, in respect to safeguarding, 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
Parents	Weduc	Two supportive emails received.	Responded and considered
Students	Email	None	None
Staff	Email	None	None
Governors	Email	None	None




Date and version control: 19 May 2020 v.4

--

## 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.

We will collect and use this information to ensure the school can undertake its remit to educate children ensuring personal safety of students, staff and visitors, protecting school buildings and its assets and to assist in managing the school (Article 6(1)(e) of the UK General Data Protection Regulation).

The lawful basis for processing is contained in the school's Privacy Notice (Student) and Privacy Notice (CCTV). It includes the following:

- Article 6 and Article 9 (Special Category Data) under Data Protection Law
- The Common Law Duty of Care
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

Going forward where there have been material changes to the way CCTV is used, the school will undertake a review of its CCTV system to ensure compliance and mitigate against 'function creep.'

When processing special category data the school will rely on the UK GDPR 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; (substantial public interest)

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.

Students, staff and visitors are already informed that CCTV is in use by signs detailing the existing scheme and its purpose, along with a contact telephone number for the current data controller (Mitie). Signage will be updated to reflect the use of a second CCTV system within the building with Summerhill School as the data controller. These signs will detail the scheme and its purpose, along with a contact telephone number for the data controller (Summerhill School)

The school has a CCTV Policy which sets out the aims of the CCTV surveillance system, positioning of cameras, signage, recording of CCTV images, viewing of CCTV images, data subject access request, system maintenance, and the twelve guiding principles of the Surveillance Camera Code of Practice.

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. The school will continue to be compliant with its Data Protection Policy.

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 consistently delivers benefits in terms of improved health and safety and security within schools. It will complement other security measures which are in place within the school.

The CCTV at Summerhill Secondary School aims to achieve the following:

- Improve the safety and security of students, staff, and visitors
- Protect the school buildings and internal infrastructure
- Improve student behaviour
- Encourage students to be prompt at the start of the lesson - Reduce vandalism
- Provide assistance in the detection and prevention of crime

The school will adhere to the principles relating to the processing of personal data contained in Article 5 specifically Article 5 (1) c "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

The school will continue to monitor incidents of behaviour and/or vandalism to determine trends within the school.

Training will be given to those who manage, operate and use the CCTV system. This will cover areas including legislation issues, monitoring, handling, disclosing, storage, deletion of information. Incident procedures, limits on system uses and disciplinary procedures if policy breached etc

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

Images will be retained for 30 days unless requested as part of an incident and then stored on archive for 12 months. The Data Management System will automatically delete the information after 30 days. Please see the school's Data Retention Policy.

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)

If data is flagged as relevant to a particular incident, it will be archived by designated staff and will then be retained for 12 months rather than being automatically deleted as described in section 15.

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?

The images will be transmitted to a Digital Video Recorder which will be housed within a secure room. Access to the room will be restricted. The images will be stored on the hard drive of the Digital Video Recorder. The Digital Video Recorder will also be kept in a locked cabinet, which ensures that the system and recordings cannot be easily interfered with should access to the office be gained.

The captured images may also be viewed live in the secure room. A designated person, i.e. a member of the Senior Leadership Team, will have access to the CCTV images. This will help to maintain site security, access control, student and staff safety.

Where appropriate authorisation has been granted to a member of staff, software would be installed on their workstation to allow the viewing and extraction of images and / or video, in response to a CCTV access request. The software will have permissions-based access controls along with the requirement for a specific password to be used to gain entry to the software. In addition, the school's ICT AUP policy will ensure that workstations are locked when users are away from their desk, so that as a minimum, two methods of authentication will be required (Windows network logon and CCTV software login) to gain access to the facility. This will be combined with physical access controls such as locked offices when not in use.

CCTV maintenance will be undertaken by Mitie as part of the school's life-cycle and maintenance agreement.

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.

The CCTV system will be capable of identifying individuals from the system and the images could be used in both criminal and civil court cases.

If a Subject Access Request is made data may be downloaded or copied for release to the data subject or a third party (in the case of a Data Protection request).

Date and version control: 19 May 2020 v.4

The system will have features that can assist in reducing privacy intrusion, i.e. blocking functions.

Each request for data must be requested via a signed data release form. In the case of the Police this can be authorised by a person at the rank of Sergeant or above using a WA170 form or equivalent.

Where requests are made to access CCTV footage the school will have a CCTV access log to record date of the request, who by, information provided, purpose, provided to third party, data securely sent, copy retained and its location.

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.

The building is of modern construction and already has lighting and other physical security measures.

Increased monitoring in person by members of staff has been explored but it is impossible for a small number of staff to continuously monitor 21 areas across a large building.

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)

The school has an annual CCTV checklist. The school also has a maintenance contract in place through Mitie.

## 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
Positioning of CCTV cameras and the issue of privacy	Remote, possible or probable  Remote	Minimal, significant or severe  Minimal	Low, medium or high  Low
Housing of CCTV cameras at a suitable height, anti vandalism measures in place	Possible	Significant	Medium
Ongoing maintenance of CCTV equipment preventing breakdowns, etc	Possible	Significant	Medium
CCTV policies and procedures not in place or not followed, leading to inconsistencies, etc	Possible	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
Maintenance and review of CCTV signage which meets requirements under the CCTV Surveillance Code of Practice	Remote, possible or probable  Probable	Minimal, significant or severe  Minimal	Low, medium or high  Low

## 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?
Positioning of CCTV cameras and the issue of privacy  Privacy issues taken into consideration when installing CCTV cameras. Cameras will be fixed in position at the time of installation and will not have PTZ feature	Eliminated reduced accepted  Reduced	Low medium high  Low	Yes/no  Yes
Housing of CCTV cameras at a suitable height, anti vandalism measures in place  Use of waterproof enclosures	Reduced	Low	Yes



--	--	--	--

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
<p>Ongoing maintenance of CCTV equipment preventing breakdowns, etc</p> <p>Contract with a maintenance company with a programme of annual maintenance checks</p>	<p>Eliminated reduced accepted</p> <p>Reduced</p>	<p>Low medium high</p> <p>Low</p>	<p>Yes/no</p> <p>Yes</p>
<p>CCTV policies and procedures not in place or not followed leading to inconsistencies, etc</p> <p>Policies and Procedures in situ including CCTV Policy, Privacy Notices and CCTV log. Training for all staff with access to system.</p>	<p>Reduced</p>	<p>Medium</p>	<p>Yes</p>


## 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:	Tim Harris / 16 <sup>th</sup> February 2022	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:	Tim Harris / 16 <sup>th</sup> February 2022	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:	None	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		<input type="text"/>
None required		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		<input type="text"/>
Consultation responses reviewed by:	Tim Harris, Vicki Poole 16 <sup>th</sup> February 2022	If your decision departs from individuals' views, you must explain your reasons.

Comments:

This DPIA will be kept  
under review by:

Vicki Poole

The DPO should also review  
ongoing compliance with DPIA.

