INVICTUS
Education Trust

CCTV POLICY

Approved by Board of Directors

To be reviewed by Board of Directors

February 2022

Contents **Page**

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) system at Invictus Education Trust operated establishments.

All cameras are monitored in school by designated staff. This policy applies to all employees, students and visitors to Invictus Education Trust premises and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance, including:

- The General Data Protection Regulations 2018 (GDPR)
- Information Commissioner's Office CCTV Code of Practice (2008)
- Human Rights Act 1998

Images of people captured on CCTV where they can be easily identified are defined as personal data under the General Data Protection Regulations 2018. This means that the Trust must meet the requirements of the Act when using CCTV.

The policy applies where open use of CCTV is intended in public areas. It does not apply to targeted or covert surveillance activities. Any operation of this kind may only be carried out with reference to the Regulation of Investigatory Powers Act (RIPA) 2000 in consultation with the Police.

2. Purpose of CCTV

The Trust uses CCTV for the following purposes:

- To provide a safe and secure environment for students, employees and visitors
- To prevent the loss of or damage to the Trust buildings and/or assets
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offending

3. Description of Systems

Invictus Education Trust use fixed and moved cameras on site. Cameras are not equipped for sound recording.

4. Siting of Cameras

All CCTV cameras will sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, students and visitors.

Cameras will 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. The Trust will make all reasonable efforts to ensure that areas outside of the Trust premises are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

5. Privacy Impact Assessment

In order to comply with The General Data Protection Regulations 2018 and ICO guidelines, a privacy impact assessment (appendix 1) should be carried out by the school's designated Data Protection Co-ordinator prior to the following actions:

- Installation of a new system
- Addition of new technology or functionality to an existing system
- The processing of more sensitive data
- The capture of images from a different location

The assessment will focus on mitigating any privacy issues linked to the use of a surveillance system.

6. Management and Access

The CCTV systems will be managed by a chosen Service Provider and designated school staff.

On a day to day basis the CCTV system will be operated by staff in school with delegated authority as appropriate.

The viewing of live CCTV images will be restricted to access by member of staff in school and Trust offices with explicit power to view images, for the reasons set out in section 2.

Recorded images which are stored by the CCTV system will be restricted to access by members of staff in school and Trust offices with explicit powers to view images, for the reasons set out in section 2.

No other individual will have the right to view or access CCTV images unless in accordance with the terms of this policy as to disclosure of images (sections 8 and 9).

The CCTV system is checked weekly by appropriate staff members in school to ensure that is operating effectively.

7. Storage and Retention of Images

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

Recorded images are stored only for a period of seven days unless there is a specific purpose for which they are retained for a longer period.

The Trust will ensure that appropriate security measures in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being located in restricted access areas
- The CCTV system being encrypted/password protected
- Restriction of the ability to make copies to specified members of staff

A log of any access to the CCTV images, including time and date of access, and a record of the individual accessing the images, will be maintained by the school.

8. Disclosure of Images to Data Subject

Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the General Data Protection Regulations 2018. Such a request should be considered in the context of the trust's Subject Access Request Policy.

When such a request is made the Data Protection Co-ordinator in school or their appropriately nominated representative will review the CCTV footage, in respect of the relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Data Protection Co-ordinator or their representative must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals then the Trust must consider whether:

- The request requires the disclosure of the images of the individuals other than the requester, for example, whether the images can be distorted so as not to identify other individuals
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made
- The process followed by the Data Protection Co-ordinator in determining whether the images contained third parties
- The considerations as to whether to allow access to those image
- The individuals that were permitted to view those images and when
- Whether a copy of the images was provided, and if so to whom, when and in what format.

9. Disclosure of Images to Third Parties

Invictus Education Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the General Data Protection Regulations 2018.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is on place.

If a request is received from a law enforcement agency for disclosure of CCTV images, the Data Protection Co-ordinator must follow the same process as in section 8. Details should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

The information above must be recorded in relation to any disclosure.

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 for the Trust should be contacted in the first instance and appropriate legal advice may be required.

10. Misuse of CCTV Systems

The misuse of CCTV systems will be dealt with under the Trust's disciplinary policy and could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

11. Review of Policy

This policy is reviewed every 3 years by Invictus Education Trust Board of Trustees. We will monitor the application and outcomes of this policy to ensure it is working effectively.

INVICTUS
Education Trust

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A DPIA is one of the ways that a data controller can check and demonstrate that their processing of personal data is compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. There are statutory requirements to carry out a DPIA in Section 64 DPA 2018 and article 35 of the GDPR.

The situations when a DPIA should be carried out, include the following:

- When you are introducing a new surveillance camera system.
- If you are considering introducing new or additional technology that may affect privacy (e.g. automatic facial recognition, automatic number plate recognition (ANPR), audio recording, body worn cameras, unmanned aerial vehicles (drones), megapixel or multi sensor very high resolution cameras).
- When you are changing the location or field of view of a camera or other such change that may raise privacy concerns.
- When you are reviewing your system to ensure that it is still justified. Both the Surveillance Camera Code of Practice and the ICO recommend that you review your system annually.
- If your system involves any form of cross referencing to other collections of personal information.
- If your system involves more than one company or agency undertaking activities either on your behalf or in their own right.
- When you change the way in which the recorded images and information is handled, used or disclosed.
- When you increase the area captured by your surveillance camera system.
- When you change or add an end user or recipient for the recorded information or information derived from it.

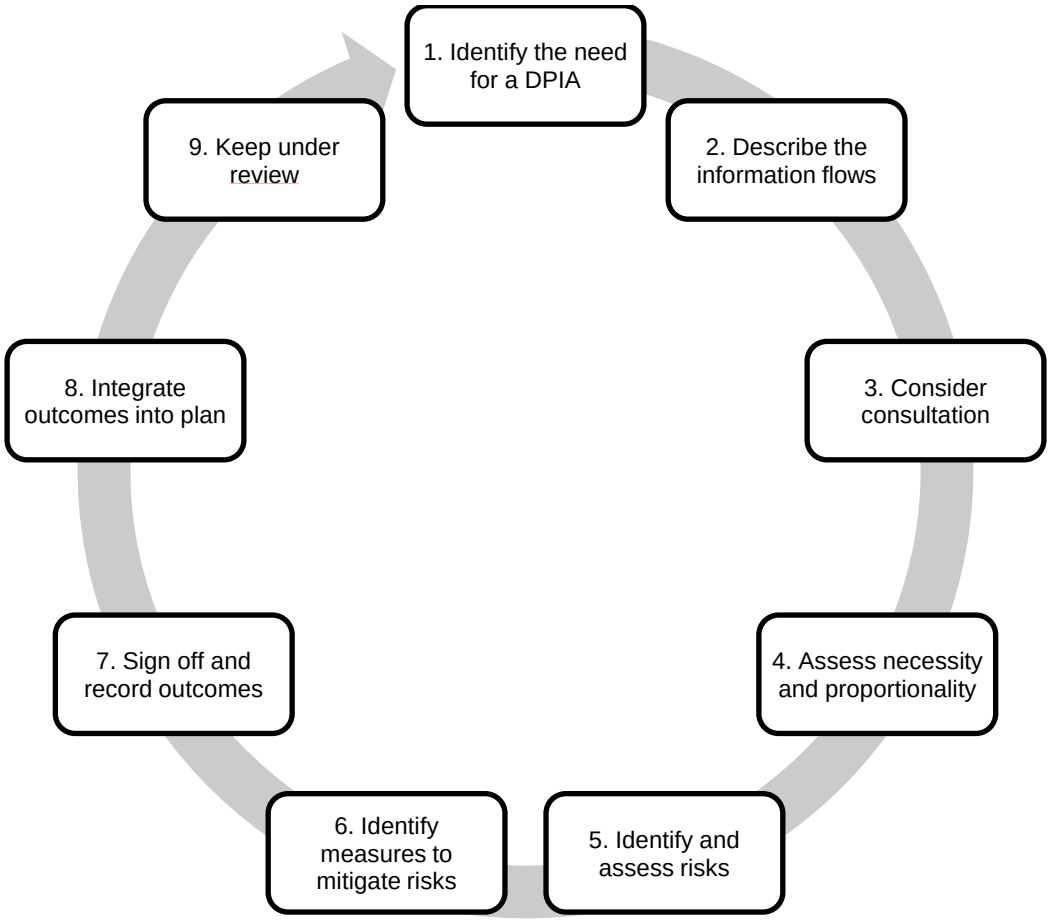
This DPIA consists of 4 parts to ensure it complies with statutory requirements in Section 64 DPA 2018 and article 35 of the GDPR:

Part 1 – Description of nature, scope, context and purpose

Part 2 – Mitigation

Part 3 – Review and Approval

STEPS IN CARRYING OUT A DPIA



Part One

Location of surveillance camera system being assessed:

Date of assessment	
Review date	
Name of person responsible	
Name of Data Protection Officer	

GDPR and Data Protection Act 2018 and Surveillance Camera Code of Practice

1. What are the problems that you need to address in defining your purpose for using the surveillance camera system?

2. Can surveillance camera technology realistically mitigate the risks attached to those problems? State why the use of surveillance cameras can mitigate the risks in practice, including evidence to justify why that would be likely to be the case.

3. What other less privacy-intrusive solutions such as improved lighting have been considered? Could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be 24/7?

4. What is the lawful basis for using the surveillance camera system?

5. Can you describe the information flows? State how data will be captured, whether it will include audio data, the form of transmission, if there is live monitoring, technologies such as automatic facial recognition etc.

6. What are the views of those who will be under surveillance? Please outline the main comments from the public resulting from your consultation – as part of a DPIA, the data controller should seek the views of those subjects who are likely to come under surveillance or their representatives on the proposition, without prejudice to the protection of commercial or public interests or the security of processing operations.

7. What are the benefits to be gained from using surveillance cameras? Give specific reasons why this is necessary compared to other alternatives.

8. What are the privacy risks arising from this surveillance camera system? State the main privacy risks relating to this particular system.

9. Have any data protection by design and default features been adopted to reduce privacy intrusion? Could any features be introduced as enhancements? State the privacy enhancing techniques and other features that have been identified, considered and accepted or rejected.

10. What organisations will be using the surveillance camera images, and where is the controller responsibility under the GDPR and Data Protection Act 2018?

11. Do the images need to be able to recognise or identify individuals, or could the purpose be met using images in which individuals cannot be identified? Explain why images that can recognise or identify people are necessary in practice.

12. How will you inform people that they are under surveillance and respond to any Subject Access Requests, the exercise of any other rights of data subjects, complaints or requests for information?

13. How will you know if the particular camera system/hardware/software/firmware being considered does deliver the desired benefits now and in the future?

14. What future demands may arise for wider use of images and how will these be addressed? Will the camera system have a future dual function or dual purpose?

15. Have you considered the extent to which your surveillance camera system may interfere with the rights and freedoms conferred under the European Convention on Human Rights? Summarise your assessment of the extent to which you might interfere with ECHR rights and freedoms, and what measures you need to take to ensure that any interference is necessary and proportionate.

16. Do any of these measures discriminate against any particular sections of the community?

Part Two

Privacy risk(s)	**Solution**	**Outcome** (Is the risk removed, reduced or accepted)	**Justification** (Is the impact after implementing each solution justified, compliant and proportionate to the aim of the camera?)

Part Three

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	
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	