Data Protection Impact Assessment (DPIA)

DPIA in relation to:
The use of CCTV in and around the school site.
Name and Position of Individual(s) responsible for DPIA:
Sarah Rayson Headteacher
Assessment date: January 2024
Review Data: January 2025

1

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. You need to check whether your processing is on the list of types of processing which automatically require a DPIA. If not, you need to screen for other factors which might indicate that it is a type of processing which is likely to result in high risk.
The use of the system is for the purpose of:- • providing assistance with ensuring and improving pupil safety and security; • protecting property; • safeguarding The pupils, staff and parents will benefit from the improved safety. The school community will benefit from the safeguarding impact of security around those admitted onto the school site and into the school building CCTV is a proven tool for detecting crimes and protecting people/property. Using CCTV can significantly reduce the time and cost on the police in investigating allegations. CCTV can realistically and consistently deliver these benefits. The GDPR places a mandatory requirement to undertake a DPIA when systematically monitor publicly accessible places on a large scale i.e. CCTV. The school has adopted The Surveillance Camera Code of Practice and Buyers toolkit. Principle 2 of the Code of Practice reflects the data protection obligations set out in data protection law. https://www.gov.uk/government/publications/surveillance-camera-code-of-practice The School has also adopted the ICO In the picture: A data protection code of practice for surveillance cameras and personal information. https://ico.org.uk/media/1043340/surveillance-by-consent-cctv-code-update-2015-jonathan-bamford-20150127.pdf

2

Step 2: Describe the processing

Describe the nature of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
How is the information collected? The system provides on-premises images, which are transmitted from cameras positioned at the front gate and front door The transmissions are received in the school office. The cameras are fixed on a particular scene to allow identification of people wishing to enter the school site. Any real-time images that are displayed in the control room environment are presented on the monitor. There are monitors located at the office workstation enabling the monitoring of incidents. They are positioned out of view of the general public. Only authorised personnel who are employed to work for the school have full operational access including moving cameras. Each camera signal is continuously recorded by way of digital video recorder. Images are stored on the hard drive of the digital video recorders (DVR), which are housed within the secure school office. The information is stored via digital recording and a data management system is in place which covers all data collected by the School surveillance system. Measures are in place to restrict and monitor access to the office by an access control system and by keypad access. Information is used to monitor those wishing to enter the school site and building and potentially prevent and detect crimes. Evidence is provided for investigation and enforcement. Individuals can requests copies of CCTV data which contains their personal information. Disclosure of data is covered by internal processes which are fully compliant with relevant legislation and codes of practice. Requests will be managed in line with the relevant legislation, including the appropriate application of any exemptions. Data management control levels are established on the system. There are password controls on the system. *Images are retained for 31 days, unless requested as part of an incident and then stored on archive for 12 months.* *The data management system automatically deletes information after 31 days by way of overwriting with new footage.* When data is required to be downloaded for disclosure to a third party (such as law enforcement or for investigation purposes or rights of access), it is done so by downloading to a disc which will then be encrypted by password protection. Each request for data must be requested via a signed data release form. In the case of the Police this is authorised by a person at the rank of Sergeant or above. All their responsibilities

3

are set out on the back page of the form which must also be signed. No data is released without both signatures.

Precautions are in place to ensure that data will continue to be collected e.g. in the event of a failure of power to cameras and DVR, which are provided by the CCTV maintenance team.

Describe the scope of the processing: What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Images captured by the cameras will be used to improve safeguarding and potentially prevent and detect crimes.
The system will be active and recording for 24 hours a day, 7 days a week.
The cameras will be recording images which will be retained for 31 days, unless requested as part of an incident and then stored on archive for 12 months.
Affected individuals will include pupils, staff, parents and visitors and may include unauthorised persons i.e. prevention and detection of crime.
The geographical areas covered by the cameras is within the boundaries of the school site, some of the school car park and public right of way outside of the school is in view of the gate camera but no residential properties can be seen.

4

Describe the context of the processing: What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been published/approved by the ICO)?
The School provides education to pupils by employing staff. Parents and carers are free to visit the premises in connection with their child/ren. Visitors such as Local authority representatives, SEN Specialists etc visit the site and play a role in the provision of pupil education. The pupils, parents, staff and visitors would not have control in the recording of images; upon valid subject access request, all parties would be able to exercise their rights to view/ obtain a copy of recorded images. There is a general expectation amongst affected individuals that recording will occur. There is signage at each camera location and the Reception sign in area highlighting the use of surveillance cameras for the purpose of safeguarding the school community. There are not any known concerns over the processing or security flaws or current issues of public concern. The system is not novel in any way. The School has adopted The Surveillance Camera Code of Practice and Buyers toolkit. The Surveillance Camera Code of Practice has been published on the School website and is approved by the ICO. The School has also adopted the ICO In the picture: A data protection code of practice for surveillance cameras and personal information.

5

Describe the purposes of the processing: What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Images captured by the cameras will be used to improve safeguarding and security and potentially prevent and detect crimes. Pupils, parents, staff and visitors will benefit from improved safety and security on site. CCTV is a proven tool in improving security and safety, detecting crimes, and perpetrators of it. Using CCTV can significantly reduce the time and costs on investigating incidents/ allegations. It is known that false allegations are made and CCTV is also useful in disproving some allegations. CCTV captures actual events and is not influenced by interpretation, or events, as seen by people who are under the influence of alcohol or drugs.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The CCTV is already in place and therefore not appropriate to now seek the views of individuals. We consulted with our Board of Governors and have consulted with our DPO. We have consulted CCTV specialists.

6

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? If appropriate, How will you prevent the use of the technology or system beyond the purpose for which it was originally intended? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The system has been established on a proper and legal basis and we comply with the Data Protection Act, Human Rights Act and Regulations of Investigatory Powers Act. Regular reviews of camera performance are undertaken to justify their need. The appropriate legal basis for processing is public task, to monitor staff and student safety. Data protection legislation gives individuals rights in respect of their data, we will support those rights where appropriate by doing the following: **Right to be informed**: there will be clear signage around the school main entrance to inform individuals of the operation of CCTV. We will also detail this in the Privacy Notices. **Right of access**: this will be supported by the school's subject access procedure. In the event of request for CCTV, we will act in accordance with data protection legislation and seek advice on any appropriate exemptions that may apply. **Right to object**: individuals have the right to object to this processing and the school will act in accordance with legislation when considering the grounds for any objection, on a case by case basis and comply with any objection where there are not deemed to be any compelling legitimate grounds to continue. **Right to restrict**: where an individual exercises their right to restrict the processing (e.g. where we no longer require the data and we receive a request to retain the data for the exercising or defence of legal claims), the school will consider the request in line with legislation and seek advice to ensure we fulfil our legal obligations. **Right to erasure:** individuals can request for their data to be erased and upon receipt of a valid request, the school will seek advice to ensure they are fulfilling their legal obligations. **Right to rectification** would not apply to the processing of CCTV **Right to data portability** would not apply to this processing

7

We have existing solutions in place, for example security fencing and an intercom linked to the school office. However, in terms of our aims CCTV is the best solution and works in conjunction with existing measures. We do inform members of the public that CCTV is in use by installing signs detailing the scheme and its purpose, along with a contact telephone number.

The system is operated by trained and vetted staff employed directly by the school. We are constantly looking at new technologies and how these will help us to improve on system delivery.

8

Step 5: Identify and assess risks

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
1) Collecting/ exceeding purposes of CCTV system Risk to individuals; New surveillance methods may be unjustified intrusion on persons privacy Compliance risk: Non-compliance with Data Protection, Human Rights legislation Corporate risk: Loss of reputation; Fines and sanctions	Possible	Minimal	Low
2) Retention of images/information for longer than necessary Risk to individuals: Owner retaining personal images/information longer than necessary Compliance risk: Non-compliance with Data Protection, Human Rights legislation Corporate risk: Loss of reputation; Fines and sanctions	Possible	Minimal	Low
3) Lack of policies and procedures and mechanisms Risk to individuals: Compliance risk: Non-compliance with Data Protection, Human Rights legislation Corporate risk: Loss of reputation; Fines and sanctions	Remote	Minimal	Low
4) Lack of signage Risk to individuals: Public not made aware that they are entering an area monitored by surveillance system Compliance risk: Non-compliance with Data Protection, Human Rights legislation Corporate risk: Loss of reputation; Fines and sanctions	Remote	Minimal	Low

9

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
1) Collection of images/information exceeds purposes	Restrict collection of images/information to identified purposes and locations. Implement appropriate technological security measures and document	Reduced	Low	Yes
2) Retention of images/information	Introduce retention periods to only keep information for as long as necessary. These are specified in the publicly available CCTV Codes of Practice/ retention policy	Reduced	Low	Yes
3) Lack of policies and procedures and mechanisms	Produce polices for handling, storage, disclosure of images/information and make them publicly available in the CCTV Codes of Practice/ School Data Protection Policy	Eliminated	Low	Yes
4) Lack of signage	Analyse area covered by CCTV system to ascertain if there is prominently placed signage at the entrance to the area monitored and also within that area. All signs to be mapped and audited regularly.	Reduced	Low	Yes

10

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Sarah Rayson	
Residual risks approved by:		
DPO advice provided:	Yvette McEwan	Legitimate basis advice
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	Head Teacher	The DPO should also review ongoing compliance with DPIA

11