Data Protection Impact Assessment (DPIA) Exemplar

DPIA in relation to:

[Insert name/reference number of project being assessed]

Installation of CCTV (overt surveillance camera systems) within the School/Academy Site

Please note: When carrying out a DPIA for the proposed CCTV system, in respect of privacy implications, you must assess each camera individually.

Please note: We recommend that a DPIA should be considered when any of the following apply:

- *you are introducing a new surveillance camera system*
- *you are changing the location or field of view of a camera or add, remove or upgrade cameras from the system*
- *you are reviewing your system to ensure that it is still justified*
- *you change or add an end user or recipient for the recorded information*

Name and Position of Individual(s) responsible for DPIA:

[Insert Name and Job title of individual(s)

Ms. Anon, Head of ICT
Mr. Smith, Head of Premises Security

Assessment date:

[Insert date]

25 May 2018

Review dates:

A DPIA is not a one- off exercise. A DPIA should be reviewed regularly ***and*** *whenever fundamental changes are made to your system (such as when cameras are added, removed or their view repositioned).*

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve, benefits 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.

1) Provide an overview of the proposed surveillance camera system. This should include the aims of the proposal i.e. why it is needed, whether there is a pressing need, what it seeks to achieve.

[The aim/use of the system shall be for the purpose of:-

●providing assistance with ensuring or improving pupil safety and security;

●protecting property;

●deterring or reducing the incidence of vandalism, graffiti and other environmental crime; and

●deterring and preventing crime.]

2) Having identified the aim, briefly explain what the benefits will be to the organisation, individuals and other parties. This could include things such as reduction of crime and offences, reduction in fear of crime, improved health and safety etc. The benefits should be capable of being measured and not anecdotal.

[The pupils, staff and parents will benefit from the improved safety and reductions/ deterrence of crime.

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.]

3) Summarise why the need for a DPIA was identified.

[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/Academy 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.

The School/Academy has also adopted the ICO In the picture: A data protection code of practice for surveillance cameras and personal information: the ICO code of practice has been published on the School/ Academy website.]

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?

1) How is the information collected? The system provides on-premises images, which are transmitted from cameras positioned in various locations throughout the premises. The transmissions are received in the CCTV Control room in the security office. Some cameras are fixed on a particular scene; others are equipped with pan, tilt, zoom facilities allowing free movement through 360 degrees.

2) Where are the real time images from the camera displayed? Any real-time images that are displayed in the secure control room environment are presented on the video wall. There are monitors located at the security officers work station enabling him to monitor incidents.

3) Who has operational access and ability to move the CCTV camera? Only authorised personnel who are employed to work within the security office have full operational access including moving cameras.

4) How are the images recorded? Each camera signal is continuously recorded by way of digital video recorder.

5) Where are the recorded images stored? On the hard drive of the digital video recorders (DVR), which are housed within the secure schools' security office.

6) How is the information stored? A digital recording and data management system is in place which covers all data collected by the School/Academy surveillance system.

7) What measures are in place to control access to the area in which the recorded images are stored? Access to the Control Room is restricted by an access control system and by intercom access for scheduled visitors. Access at the remote sites is again restricted by an access control system to each room.

8) How is information used? Information is used to monitor pupil safety and security, protect property and 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.

9) How is access gained to the recorded images? Data management control levels established on system. Password controls on system. Hardcopy requests for images required.

10) How long are the images retained? 31 days, unless requested as part of an incident and then stored on archive for 12 months.

11) How is information deleted? The data management system automatically deleted information after 31 days.

12) When data is downloaded or copied for release to a third party how is information recorded? CD ROM, DVD or portable hard drive

13) What processes are in place to ensure that data protection responsibilities are understood *by persons receiving the data? 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 are set out on the back page of the form which must also be signed. No data is released without both signatures.*

14) What 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? An UPS system in operation.

UPS - An uninterruptible power supply or uninterruptible power source is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails.

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?

Explain what data and/ or images will be captured, where the images will be collected from, from whom/ what is the information collected and why is it being collected.

[Images captured by the cameras will be used to improve/ monitor pupil safety and security, protect property and prevent and detect crimes.

The system will be active i.e. recording 24 hours [or specific time periods].

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 system covers external school premises including the School/Academy play area and sports fields and internal cameras are also sited at premises entrances.]

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/Academy provide education to pupils by employing staff. Pupil parents 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.

There are not any known prior concerns over the proposed processing or security flaws or current issues of public concern. The system is not novel in any way.

The School/Academy has adopted The Surveillance Camera Code of Practice and Buyers toolkit. The Surveillance Camera Code of Practice has been published on the School/Academy website and is approved by the ICO.

The School/Academy has also adopted the ICO In the picture: A data protection code of practice for surveillance cameras and personal information: the ICO code of practice has been published on the School/ Academy website.]

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?

Include here why the surveillance or monitoring system is needed, whether there is a pressing need, what it seeks to achieve, whether there is a proper legal basis for collecting this information, etc.

Images captured by the cameras will be used to improve/ monitor pupil safety and security, protect property and prevent and detect crimes.

Pupils, parents, staff and visitors will benefit from improved safety and reductions in crime.

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?

[We need to seek /have already sought the views of parents and staff; this was sought by way of staff meetings and parent newsletter/forum.

We shall need to involve/ have involved our security personnel who are employed at the School/ Local Authority, our Board of Governors/ Academy Trust.

We have consulted/ plan to consult with our DPO.

We plan to consult/ have consulted CCTV specialists.]

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 legal bases for processing are legitimate interest and public interest. *We have existing solutions in place, for example security fencing and/ or improved lighting. 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 must be capable of identifying individuals, as footage from the system will be used in both criminal and civil court cases. If the system did not have this capability it would not be fit for purpose.* *The system will be delivered/ operated by trained and vetted staff employed directly by the School/Academy. We are constantly looking at new technologies and how these will help us to improve on system delivery.]*

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: No public availability of CCTV code of Practice which details how personal data handled, stored, disclosed etc.* *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*

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*

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	*Head of School/ Academy* *Board of Governors* *Head of ICT Department*	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	*Head of School/ Academy* *Board of Governors*	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	*The School DPO Service (Warwickshire Legal Services)*	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: *No high risks or residual high risks were identified.* *All the low risks which were identified have been reduced or eliminated. The School/ Academy must ensure they have an appropriate procedure in place to monitor and ensure the Options identified in Step 6 are applied.* *There is no requirement to consult with the ICO.*		
DPO advice accepted or overruled by:	*Head of School/ Academy-Accepted* *Board of Governors - Accepted*	If overruled, you must explain your reasons
Comments: *N/A*		
Consultation responses reviewed by:	*Head of School/ Academy* *Board of Governors* *Head of ICT Department*	If your decision departs from individuals' views, you must explain your reasons
Comments: *N/A*		
This DPIA will be kept under review by:	*Head of School/ Academy*	The DPO should also review ongoing compliance with DPIA

	Head of ICT Department	