Data Protection Impact Assessment (DPIA)

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.
Our project aims are to deter crime and assist in the detection of criminal offences, accidental damage/injury and antisocial behaviour against our property and equipment, and the personal property of employees, contractors, visitors and members of the public. We also aim to provide evidence for potential insurance claims. We wish to reduce crime and anti-social behaviour towards our property and improve the safety and security of our business. We have installed 16 cameras, 2 on each corner of our 2 buildings. These cameras are pointed at our buildings in order to monitor criminal activity, accidental damage/injury and antisocial behaviour and crime prevention. See site plan. There could be legitimate concerns from employees, local residents and local businesses regarding the use of CCTV around our property. By ensuring compliance with current legislation we hope to show that CCTV camera system is only used for the detection and reduction of crime, accidental damage/injury, antisocial behaviour and activities that ultimately assist the public. We have not received any complaints regarding the use of CCTV.
Step 2: Describe the processing
Describe the nature of the processing: How will you collect, use, store and delete data? What is the course of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?
The data will be collected via our video surveillance cameras. The data will be stored for 14 days, after which it will be automatically deleted. The video footage is captured by the integral camera and stored on an internal password protected and encrypted hard drive. The course of the data is as follows: Collect images If no to criminal activity, accidental damage/injury or antisocial behaviour delete images after one month If yes to criminal activity, accidental damage/injury or antisocial behaviour scan images and forward to police and/or insurance company if relevant to their investigation If not relevant to police investigation, then delete image after 28 days. The data will only be accessed on an ad hoc basis. The data will not be shared unless needed by the police and/or insurance company to aid in their investigation. There is no high risk processing involved.

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?

The video footage is captured by the camera and transmitted via our digital network to our Network Video Recorder (NVR) that is password protected and situated in our IT office onsite.
The stored footage has a retention period of 14 days, after which the NVR automatically overwrites the footage thus deleting it. If the footage is deemed to be of evidential value this can be quarantined by our IT.

All quarantined footage will be deleted after 28 days after sharing with the police and/or insurance company. When such data is retained, it will be retained in accordance with our Data Protection Policy. Information including the date, time and length of the recordings, as well as the locations covered, and groups of individuals recorded, will be recorded in our system log book.

See camera placement plan attached.

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 they have been approved)?

It is very important that the system is capable of identifying individuals as footage from the system may be used in court. If individuals are not identifiable then the system would not be fit for purpose.

Individuals have the right to access personal data D.K. Holdings Limited holds on them as per our Data Protection Policy. Where images are provided to third parties, practicable steps will be taken to obscure images of non-relevant individuals.

The surveillance cameras will be pointing at our property and not at the general public unless it is impractical. The only time that this information will be accessed will be when there has been an incident and our IT department will check to see if there is an individual(s) captured as the person(s) responsible. The police will be contacted if a person carrying out the crime has been detected.

There are other security cameras operating in this area but not near our building.

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?
The CCTV system will act as a crime deterrent and add security for both premises and equipment. CCTV will provide high-quality evidence of those involved in crime and antisocial behaviour and may deter some of those involved from participating in crime in the future. CCTV will also provide high-quality evidence of circumstances of accidental damage/injury.
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?
A work notice has been placed in every department letting employees know that CCTV is being installed. A notice has been erected for the general public to be aware of the presence of CCTV.
Step 4: Assess necessity and proportionality
Describe compliance and proportionality measure, 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? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individual? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
We believe that the lawful basis for processing is in its legitimate interests. Data captured for our purposes will not be used for any commercial purpose. Our objectives are to protect D.K. Holdings Limited buildings and equipment and the personal property of employees, contractors, visitors and members of the public. Also to support the police and community in preventing and detecting crime/antisocial behaviour, assisting in the identification and apprehension of offenders and providing evidence in relation to accidental damage/injury. The system manager will check and confirm that the system is properly recording and that cameras are functioning correctly on a regular basis. Staff authorised by D.K. Holdings Limited will conduct routine supervision of the CCTV system. Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access by unauthorised persons. Images will be stored for 14 days and automatically over-written unless D.K. Holdings Limited considers it reasonably necessary for the pursuit of the objectives outlined above or if lawfully required by an appropriate third party such as the police or local authority. Where data is retained, it will be retained in accordance with the DPA and our Data Protection Policy. Information including the date, time and length of the recordings as well as the locations covered, and groups of individuals recorded, will be recorded in the system log book, accessed only by authorised persons. Individuals have the right to access personal data D.K. Holdings Limited holds on them as per our Data Protection Policy. D.K. Holdings Limited will require specific details including at least the time, date and camera location before it can properly respond to such requests. This right is subject of certain exemptions from access including in some circumstances where others are identifiable. The system manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and legitimacy of the request. Where images are provided to third parties wherever practicable steps will be taken to obscure images of non-relevant individuals. See our CCTV Policy and Data Protection Policy.

Step 5: Identify and assess risks			
Describe the 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**
Personal data retained for longer than necessary or personal data collected and stored unnecessarily	Remote	Minimal	Low
Disclosure of personal data to unauthorised persons or agencies	Remote	Minimal	Low
Unauthorised third party access to images	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 step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced or accepted	Low, medium or high	Yes/no
Personal data retained for longer than necessary or personal data collected and stored unnecessarily	Automatically deleted after 14 days	Eliminated	Low	
Disclosure of personal data to unauthorised persons or agencies	Authorised persons only have access to recorded data	Accepted	Low	
Unauthorised third party access to images	Encrypted data and password protected	Accepted	Low	

Step 7: Sign off and record outcomes				
Item	**Name/Date**		**Notes**	
Measures approved by:	Peter Goodhew Darren Mills		Integrate actions back into project plan, with date and responsibility for completion	
Residual risks approved by:	Darren Mills		If accepting any residual high risk, consult ICO before going ahead	
DPO advice provided:			DPO should advise on compliance, step 6 measures and whether processing can proceed.	
Summary of DPO advice:				
DPO advice accepted or overruled by:			If over ruled, 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:			The DPO should also review ongoing compliance with DPIA	
Step 8: Integrate outcomes into plan				
Insert company process for integrating processing into existing plans				
Our Data Protection Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject including CCTV recordings. We commit to the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data. We adhere to the principles relating to the processing of Personal data set out in the GDPR which require personal data to be: (a) Processed lawfully, fairly and in a transparent manner (the Lawfulness, Fairness and Transparency principle); (b) Collected only for specified, explicit and legitimate purposes (the Purpose Limitation principle) (c) Adequate relevant and limited to what is necessary in relation to the purposes for which it is processed (the Data Minimisation principle); (d) Accurate and where necessary kept up to date (the Accuracy principle);				

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes of which the data is processed (the storage Limitation principle);
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (the Security, Integrity and Confidentiality principle);
(g) Not transferred to another country without appropriate safeguards being in place (the transfer Limitation principle); and
(h) Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (the Accountability principle).

Step 9: Keep under review

Insert company policy for review dates on processes

Please see our Data Protection Policy and CCTV Policy.
We have an annual GDPR audit carried out by JXG Management Solutions Ltd