Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	Brackley Town Council
Subject/title of DPO	Brackley Town Council CCTV Scheme
Name of controller contact	Kathy Hale/Mark Yates

Step 1: Identify the need for a DPIA

Explain broadly what 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.
Brackley Town Council is a medium to large Town Council responsible for the management and operation of three community buildings, two public toilets, works depot, office and a range of other community assests. This Data Protection Impact Assessment (DPIA) has been completed to identify and assess any data protection risks arising from the use of CCTV systems installed across these sites. The primary purpose of the CCTV is to deter and detect crime, promote public safety, protect Council property, and assist in the investigation of incidents. The processing involves the continuous collection of visual personal data through recording, secure storage of footage, controlled access by authorised personnel, and disclosure to law enforcement or other relevant authorities when necessary. The need for a DPIA was identified because the CCTV system involves systematic monitoring of publicly accessible areas on a large scale, which can have a potential impact on individuals' privacy rights. By carrying out this assessment, the Council aims to minimise risks to individuals, demonstrate compliance with the UK GDPR, and inspire public confidence through clear communication and transparent data protection practices.

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?

Personal data is collected continuously via fixed CCTV cameras installed at Council-owned sites. The cameras capture video images but do not record sound.

Footage is stored securely on a digital recording system located on Council premises. Recordings are retained for a maximum of 30 days, after which they are automatically overwritten, unless footage has been specifically downloaded in response to an incident, complaint, or formal request for disclosure.

Where footage is downloaded for evidential or investigative purposes, it is stored securely in a restricted-access folder and retained only for as long as necessary in accordance with our CCTV policy and retention schedule.

Access to live feeds and recorded images is restricted to authorised Council staff who have received appropriate training in data protection and CCTV operation.

Footage will not be shared with third parties except:

- when required by law (e.g., to assist the police or other enforcement authorities in the investigation of crime),
- to support legal proceedings, or
- where disclosure is otherwise permitted under the Data Protection Act 2018.

The source of all personal data is the CCTV cameras themselves; no other data sources are used in conjunction with the CCTV system. The types of processing which may be considered high-risk include systematic monitoring of public areas and the potential for capturing special category data incidentally (e.g., where footage reveals health information or other sensitive details).

A supporting CCTV Policy are in place to ensure compliance with data protection principles and to minimise risks to individuals' rights and freedoms.

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 CCTV system captures visual personal data in the form of video surveillance footage only. No audio recording takes place. The cameras record continuously during operational hours. The nature of the data is general visual imagery of individuals in public areas and Council premises within the parish of Brackley. The system does not intentionally collect special category data (such as health data) or criminal offence data, although such data may be captured incidentally if an individual's behaviour or circumstances are recorded (for example, if an incident occurs). Amount and frequency of data collection: • Footage is recorded continuously whenever the cameras are active. • This results in a significant volume of data collected daily, although the footage is only reviewed or retrieved when necessary (e.g., an incident, complaint, or lawful request). **Retention periods:** Footage is retained for 30 days before automatic deletion unless downloaded due to an incident or concern. **Individuals affected:** Members of the public, staff, volunteers, contractors, and visitors to these premises and surrounding areas. The number of individuals is variable, depending on public use of the sites. Although the CCTV system does not target any specific individuals or groups, it records everyone who enters the coverage areas.

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 approved)?
The CCTV systems are installed for the purposes of protecting Council property and assets, deterring and detecting criminal activity, promoting public safety, and supporting the security of staff, volunteers, and visitors. The nature of the Council's relationship with individuals is as the owner and manager of public buildings and community facilities. People entering the premises are members of the public, Council staff, volunteers, contractors, or visitors. Individuals have limited direct control over whether their images are captured while in these public areas, as the CCTV operates continuously. However, clear signage is in place to inform them that CCTV monitoring is taking place, the purpose of the monitoring, and the Council's contact details. It is reasonable for individuals to expect that CCTV will be used in such locations, as this is standard practice in publicly accessible Council facilities to promote safety and deter anti-social behaviour. Children and potentially other vulnerable individuals (such as older people or people with disabilities) are likely to be captured in the footage. This has been considered in assessing the proportionality of the system and the need for appropriate safeguards (e.g., restricted access to footage, clear retention periods, and staff training). There are no known prior concerns or incidents relating to misuse or security flaws in the operation of the Council's CCTV systems. The use of CCTV is not novel or unusual in this context and reflects common practice across similar local authority settings. The current state of technology is well-established and involves the use of standard digital video recording systems. There are no known specific current issues of public concern at these sites that would impact the justification for CCTV. However, the Council will continue to monitor community feedback and consider any concerns raised about privacy or data protection. The Council is not currently signed up to an approved code of conduct or certification scheme under Article 40 of the UK GDPR, as no relevant approved codes exist for this area at present. However, the Council adheres to the ICO's CCTV Code of Practice and relevant guidance from the Surveillance Camera Commissioner

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 purpose of the CCTV processing is to: • Deter and detect anti-social behaviour, vandalism, and criminal activity on Council-owned premises. • Promote public safety and provide reassurance to members of the community, staff, volunteers, and visitors using these facilities. • Protect the Council's property and assets from damage, theft, or misuse. • Support local crime prevention measures and assist law enforcement agencies, where appropriate, by providing evidence in connection with criminal investigations or legal proceedings. • Improve the Council's ability to manage liability and insurance claims by demonstrating that reasonable and proportionate steps have been taken to safeguard the premises. The intended effect on individuals is minimal, as the system is not used to monitor individuals' activities beyond what is necessary to achieve these purposes. The cameras are positioned to cover key areas where incidents are more likely to occur and are not used for general tracking or profiling of individuals. The benefits of this processing include: • Increased confidence among the public that the Council is taking active steps to maintain a safe environment. • Enhanced security and safety for staff working at Council premises. • Reduced incidence of anti-social or criminal behaviour through visible deterrence. • Improved ability to investigate incidents and support enforcement action if necessary. • Protection of public funds by reducing repair costs and potential claims arising from vandalism or other criminal activity.

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?
Given the nature of the CCTV system—covering public areas for crime prevention, safety, and asset protection—the Council has assessed that formal consultation with individual members of the public is not necessary at this stage. CCTV used in these settings is standard practice and generally expected by those using the facilities. Public awareness and transparency are ensured through: • Prominent signage clearly indicating CCTV monitoring and explaining its purpose • Information available via the Council's website and privacy notices. The Council will continue to remain open to receiving feedback or concerns from members of the public about the operation of the CCTV system and will review any comments or complaints raised. Within the organisation, the following stakeholders have been or will be involved in the assessment and management of data protection risks: • The Town Clerk and management team responsible for overseeing building and asset security. • The Council's Data Protection Officer, who has reviewed the DPIA and associated policies. • Facilities staff authorised to access and manage CCTV systems. Where necessary, the Council may consult its CCTV system suppliers or maintenance contractors (as data processors) to ensure technical and organisational safeguards are robust and up to date. At this time, the Council does not consider it necessary to seek external information security or surveillance technology experts, as the system is not novel, and the relevant standards and guidance (such as the ICO CCTV Code of Practice) are well established. • This position will be kept under review, particularly if: • The system is expanded significantly • New technologies are introduced (e.g., facial recognition) • There are any public concerns or complaints.

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? How will you prevent function creep? 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 use of CCTV is considered necessary and proportionate to achieve the Council's legitimate aims of:

- Protecting its property and assets
- Ensuring public and staff safety
- Deterring and detecting crime and anti-social behaviour
- Supporting investigations by law enforcement where appropriate
- Reducing the risk of liability or false claims Lawful basis for processing:

The lawful basis under the UK GDPR is:

- Article 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Where applicable, processing may also rely on:

The system is not used for any purpose that would require special category data or criminal offence data as defined under Articles 9 and 10.

Proportionality and alternatives considered:

The Council has considered whether the same purposes could be achieved in a less intrusive way (e.g. physical patrols, improved lighting, increased signage). However, these methods alone would not offer the same level of deterrence, evidential value, or coverage, especially outside staffed hours. CCTV is therefore viewed as a complementary and proportionate solution.

Preventing function creep:

The Council will prevent function creep by:

- Operating the system strictly in accordance with the CCTV Policy
- Limiting use to the original purposes only (crime prevention, safety, asset protection)
- Reviewing any proposed changes in use through the DPIA process
- Ensuring staff are trained and aware of restrictions on use

Data minimisation and quality:

- Cameras are placed only where necessary to achieve the stated purposes
- No audio is recorded
- Footage is retained only for the set retention periods (30 days) unless required for a specific incident.
- Access is restricted to authorised staff only

- Regular checks are conducted to ensure the system is functioning properly and that time/date stamps are accurate.

Supporting individual rights:

- Individuals are informed via clear signage at all CCTV locations
- The Council provides a CCTV privacy notice online and on request
- Individuals may submit a Subject Access Request (SAR) to request copies of footage involving them
- Requests are handled in accordance with data protection law, and redaction measures are in place to protect the rights of third parties

Processor compliance:

- Any external providers (e.g. CCTV maintenance contractors) are subject to written agreements outlining data protection obligations
- Processors are not permitted to access footage unless necessary for system maintenance or troubleshooting, and only under Council supervision
- Regular reviews are undertaken to ensure processors comply with these requirements

International transfers:

- No data is transferred outside the UK or EEA. All footage is stored on local systems maintained within the UK.

Step 5: Identify and assess risks

10

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
Data breach – video footage released to the general public	Remote	Minimal	Low
Hacking or system compromise	Remote	Minimal	Low
System failure	Possible	Minimal	Low
Legal or regulatory action if found non-compliant with data protection laws – clear signage and policy implementation with staff training	Possible	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**
Data Breach	All staff to undertake data protection training with only named, authorized staff permitted to download material	Accepted	Low	Yes
	Live action feed is for staff security whilst lone working and for immediate escalation/ request for support in the event of an incident.	Accepted	Low	Yes
Hacking or system compromise	Non sensitive data contained within recorded footage. App downloaded onto named, key staff work mobile devices. No audio recording.	Accepted	Low	Yes
	Cameras placed in expected locations.	Accepted	Medium	Yes
System failure	Daily inspection of recordings. CCTV for preventative measures therefore impact of failure low. Outage log to be maintained.	Accepted	Medium	Yes
Legal non compliance	CCTV policy in place, staff training, signage, outage log, no audio recording and privacy notice published to explain how data is used.	Accepted	Low	Yes

12

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Lesley Sambrook Smith/Deputy CEO Northants CALC/ 15/9/25	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The DPIA is comprehensive and the risk review has considered all risks and they are all at an acceptable level with mitigations being provided. The lawful basis for processing has been correctly identified and I can see no issues with this DPIA.		
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 kept under review by:		The DPO should also review ongoing compliance with DPIA