Angus Council

Data Protection

Data Protection Impact Assessment

Project: Use of body cams and mobile CCTV
Waste
Roads and Transportation

"Privacy by Design"
Office of the Information Commissioner

Data Protection Impact Assessment

Name or Description of Process

Use of body worn cameras and mobile CCTV (Waste and Roads & Transportation)

Date Assessment Approved **Review Date**

5 February 2019

Approvals	**Signatures**
Senior Responsible Managers	Head of Service, Communities & Head of Service, Infrastructure
Process Owner	Senior Community Safety Officer (Enforcement) & Waste Services Co-ordinator
Data Protection Officer	[redacted] Manager – Legal Team 2

Signatures:

[redacted]

Head of Communities	5 February 2019
Head Infrastructure	5 February 2019

[redacted]

[redacted]

Section 1 – Description of the Processing

What is the purpose of the processing? What is it intended to achieve? Who will benefit from the processing?
Body worn cameras (BWC) will be utilised by Community Enforcement Wardens, Recycling Centre Attendants and Waste Management Inspectors in the course of their duties. • Evidentiary purposes when issuing Fixed Penalty Notices • Evidentiary purposes when issuing Penalty Charge Notices • Crime prevention and public safety • Prevention and protection of Angus Council employees and members of the public from violence and aggression Mobile CCTV (MCCTV) will be used for: • Crime prevention • Evidentiary purposes for environmental crimes such as fly tipping
Who are the data subjects (e.g. customers, employees)?
BWC: Employees, members of the public MCCTV: members of the public, potential offenders
Does the data include personal data concerning individuals other than the data subject? If so, list the groups affected (e.g. next of kin).
BWC: Yes, potentially but unlikely. Vehicle Registration Marks (VRMs) will possibly be captured. MCCTV: Potentially but unlikely - directed surveillance at hotspots to record commission of offences, including VRM for identification.
What personal data will be processed? List personal identifiers, general categories of information, and any special categories as defined by the GDPR.

Name Address Date of Birth VRMs Image Voice (BWC only)	Secondary images may be captured including: Health (disability) Political persuasion Ethnicity However this information is not processed

How often will the processing typically occur in relation to an individual data subject? Is it part of a larger process? Provide an overview of the larger process.
Body cameras are utilised on a daily basis and Mobile CCTV is used in [redacted] identified as high risk to fly tipping (for approximately 4 weeks at a time). If an image/sound is required for evidentiary purposes it will be retained until the conclusion of the case. After this the recording will be deleted. Recordings not required for evidentiary purposes are automatically deleted within 30 days. Those recordings required for evidentiary purposes require to be marked as such in order that they are not part of the software's automatic deletion programme.

Describe each step of the processing. You should include what is done, who carries out each process step, and how the processing is done (e.g. paper record, computer system, photograph, etc.). An information processing flowchart may assist.		
What is done	By whom	How it is done
Image/sound is recorded.	Body cam operative MCCTV	Activation of equipment
Recordings downloaded from camera to laptop.	Line manager of operative	Connect to stand alone laptop with encrypted software
Recordings are reviewed and retention determined.	Line Manager	Evidentiary files are marked for retention. Files may also be marked for staff training purposes.
Recordings not marked for retention are deleted.	Software	Automatically
Recordings marked for retention are deleted.	Line Manager	Manually once case is closed.
Recoding may be passed to partner agencies (e.g. breach of the peace during issue of PCN may be shared with Police Scotland).	Line Manager	Download to encrypted USB. Issuing and receiving officer sign declaration of transfer of information.
Recording utilised for staff training purposes.	Line Manager	Recording is played to demonstrate examples of good/bad practice thereafter deleted.
Request from data subject to view recording.	Line Manager	Data subject attends council office to review footage.
Recording utilised for disciplinary purposes – would include sharing with HR and others included in the process (e.g. union rep).	Line Manager	Recording is played to employee and those involved in investigation.

Signage is in place at recycling centres to advise of the use of CCTV and this will be renewed to include information about body worn cameras. Protocols are in place detailing who can access/delete and pass footage to a third party.	Service Leader (Environmental Services) See attached Recorded Data Management Protocols	Signage is reviewed See attached Recorded Data Management Protocols

How long will the information be stored? If it will be stored for a period after it is required for processing what is the basis for that retention period?

Information will automatically delete after 30 days for waste body camera systems and mobile CCTV. This extends to 90 days for community enforcement system due to the PCN appeal procedure timeframe.

Recordings required for evidentiary purposes will be retained until closure of the case. It is not possible to specify an exact time limit.

What systems (electronic or paper based) will be used to store and process the data? Include descriptions of the hardware, software, paper filing systems, etc.

Waste

[redacted] body cameras and [redacted] Manager software.

[redacted] CCTV camera and [redacted] Cloud Management (TBC)

Community Enforcement

Reveal body cameras and [redacted] software.

Software is held on Angus Council encrypted laptops.

Who will have access to the personal data during processing? List the staff roles and the legitimate reasons for access.

See attached Recorded Data Management Protocols

Senior Community Enforcement Wardens (x2) – reviewing footage and determining the need for retention or deletion.
Community Safety Assistant (x1) – physical download of files in absence of SCEW and SCSOE
Senior Community Safety Officer (Enforcement) (x1) – reviewing footage and determining the need for retention or deletion

Team Leader – Waste Strategy & Compliance – downloading, reviewing footage

and determining the need for retention and deletion, passing to partner agencies
Waste Services Co-ordinator (x1) – downloading, reviewing footage and determining the need for retention and deletion, passing to partner agencies
Assistant Operations Manager (x1) –downloading, reviewing footage and determining the need for retention and deletion, passing to partner agencies

Police Scotland – [redacted] for use in criminal proceedings

Procurator Fiscal - [redacted] for use in criminal proceedings

Community Enforcement Wardens (x12), Recycling Centre Attendances (x25) and Waste Management Inspectors (x4) – for training purposes only.

Angus Council employees as required in disciplinary proceedings and any other third party involved as outlined in the disciplinary process.

Will the data be shared with third parties? If so, list the parties and any limits to the range of personal information which will be shared.

Third Party Recipient	**Limitations to Information Shared**
Police Scotland	Criminal proceedings – footage for evidence [redacted]
Procurator Fiscal	Criminal proceedings – footage for evidence [redacted]

Section 2 – Proportionality and Necessity of the Processing

What measures have been taken to ensure the processing will be specific, explicit and legitimate?

The nature of the roles determine when the recording devices are used. Enforcement staff will activate their cameras during every direct interaction with the public as their role means it is more likely that they will encounter confrontational situations.

Recycling Operatives and Waste Management Inspectors will use the recording devices when they feel that an interaction may be becoming threatening.

MCCTV will be aimed at hotspot areas only, and clearly signed. The angle and area covered will be considered to limit intrusion onto other areas.

On what legal basis or bases is the data to be processed?

6(1)(e) – Public Task

6(1)(c) – Legal Obligation

Environmental Protection Act 1990

Dog Fouling Act (Scotland) 2004

Road Traffic Regulation Act 1984

Road Traffic Act 1991

Disabled Persons' Parking Places (Scotland) Act 2009

Health & Safety at Work etc. Act 1974

If the rights of data subjects eg *right to be informed, right of erasure, right of access, right of rectification* etc (see section 3 below) are restricted by the legal basis for processing, what reasons are there for considering the processing to be proportionate?

Signage advising of the use of CCTV is placed on entry to each of the seven burghs in Angus and larger villages. Additionally signs are placed at the entrance to recycling centres. Data subjects are informed that they will be recorded at the point the operative makes the decision to activate the device. Within waste the camera records on a constant 2 minute loop to enable a recording to capture the previous 120 seconds of footage.

Where MCCTV is deployed, any area being monitored will have signage advising of its use.

What reasons are there for considering the processing is necessary to achieve the stated purpose and that there are no other reasonable ways to achieve that purpose?

We determine that the processing of the information is necessary to achieve

- Evidentiary purposes when issuing Fixed Penalty Notices
- Evidentiary purposes when issuing Penalty Charge Notices
- Evidence of fly tipping taking place
- crime prevention and public safety
- prevention and protection of Angus Council employees and members of the public from violence and aggression

as this removes the need for corroboration and removes ambiguity, providing quality, accurate evidence.

What measures have been taken to ensure the personal information collected is both adequate to achieve the purpose of the processing and limited to on that information which is necessary to achieve the purpose?

Date stamp and time is mandatory on all devices and is checked on a regular basis to ensure accuracy. Equipment is in good repair and a replacement programme is in place. In community enforcement, operators can view the date and time at the time of recording and the data subject can see what is being recorded in real time.
What measures have been taken to ensure the information is accurate and is kept up to date?
Not applicable.

Section 3 – Protecting Data Subject Rights

How will the right of the subject to be informed be met?
Signage and statement of intent to record.
If data subjects retain a right of access under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Data subject will be required to submit a request to view the footage via ACCESSLine.
If data subjects retain a right to rectification under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If data subjects retain a right to erasure under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Detail contained within the privacy notice if a data subject wishes the footage to be erased prior to the 30 day automatic delete. This only applies if footage is not required for evidential purposes.
If data subjects retain a right to data portability under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?

Not applicable.
If data subjects retain a right to restrict processing under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If data subjects retain a right to object under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If some of the processing will be carried out by third party data processors, are there adequate contracts or service level agreements in place specifying the requirements for the processes undertaken, data sharing limitations, security requirements, and duties in relation to data subjects' rights? What arrangements are in place for monitoring compliance and reporting breaches?
Information Sharing Protocol with Police Scotland is in place. Body cameras [redacted] Laptops [redacted] It is therefore highly unlikely that a breach would occur - [redacted] Any other breach would be a deliberate act and would be evident from the audit log.
Is the personal data held and processed only within the UK or the European Economic Area? If not, what safeguards are in place to ensure the security, integrity and confidentiality of the data?
Yes
If the processing covered by this DPIA is considered to pose a high risk in the absence of mitigation, has there been prior consultation with the Information Commissioner? What was the outcome of that consultation?
The information referred to in this DPIA is not deemed high risk as there are mitigation processes in place as detailed in this DPIA.

Section 4 – Data Protection Risk Assessment

Use this section to identify the risks to the rights and freedoms of data subjects posed by the processing covered in this DPIA.

There are four main sources of risk which need to be considered:

- Illegitimate access to data
- Undesired modification of data
- Disappearance or destruction of data
- Inappropriate or uncontrolled sharing of data

For each of these categories, identify where in the processing the risk of a breach might arise and how it might arise. For each risk you need to quantify the:

- Likelihood of a breach occurring
  (1=negligible, 2=low, 3=moderate, 4=high, 5=extremely likely)
- The severity of the impact of a breach on the data subjects rights and freedoms
  (1=negligible, 2=minor, 3=moderate, 4=major, 5=catastrophic)
- The overall risk score (likelihood multiplied by severity)

You should then list the actions you will take to mitigate or eliminate each risk. The aim is to demonstrate that you have designed the process in such a way as to prevent or minimise the risk of a breach occurring.

If the overall score for any risk is 15 or more then you must seek prior consultation with the Data Protection Officer before implementing the processing covered by this DPIA.

Add rows to the tables as necessary.

1.1 *Illegitimate Access*

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Recording footage accessed by unauthorised staff.	2	2	4	[redacted]
Footage [redacted] or transfer to third party.	1	2	2	[redacted]

1.2 *Undesired Modification*

Risk Description	Likelihood	Severity	Score	Mitigation Actions

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Software does not allow for modification and information cannot be accessed directly from cameras.	1	1	1	

1.3 Disappearance or Destruction

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Footage is deleted in error.	1	1	1	[redacted] deletion process in place.

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Footage is deleted intentionally.	1	1	1	System audit in place and would result in disciplinary action.

1.4 Inappropriate or uncontrolled sharing

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Recorded footage is distributed to a wider audience.	1	2	2	Only authorised officers (as detailed in the attached protocols) to view footage. Any inappropriate sharing would result in disciplinary action.

Section 5 – Data Protection Officer's Advice

Whilst this processing may be considered intrusive to an individual's privacy and may impact on the rights and freedoms of data subjects, I consider that sufficient controls are in place to mitigate the risks arising from this processing. In particular, it will be important for training to be carried out, guidance provided and the protocols followed to ensure that the controls are effective.

I have advised the service of the requirement to take account of the ICO Code of Practice for surveillance cameras and personal information.

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

as following the recommendations in this code will:

- help ensure that those capturing individuals' information comply with the DPA and other relevant statutory obligations;
- contribute to the efficient deployment and operation of a camera system;
- mean that the information captured is usable and can meet its objectives in practice;
- reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- re-assure those whose information is being captured; and
- help inspire wider public trust and confidence in the use of CCTV.

The information provided in this DPIA would indicate that the processes put in place shall ensure compliance with the principles underlying the code.

Final decision if Data Controller's advice is contrary to the proposed processing

Section 6 – Outcome of Consultation with Data Subjects (if applicable)

Data Protection

Data Protection Impact Assessment

Project: Supply, Install and Maintain Public Space CCTV for Smart City/ Town Management

"Privacy by Design"
Office of the Information Commissioner

Data Protection Impact Assessment

Name or Description of Process

Supply, installation and maintenance of a CCTV System for Smart City/ Town Management for Angus Council in collaboration with Dundee City Council, Perth & Kinross Council and Police Scotland.

Date Assessment Approved	Review Date
7 January 2020	7 January 2021
23 August 2021	23 August 2022

Approvals	Signatures
Senior Responsible Manager	Director of Service Infrastructure
Process Owner	System controller: Team Leader Property Maintenance Data Controller & Processor: Police Scotland
Data Protection Officer	Manager Legal Team 2
Information Officer	Manager Property Asset

Document Control Sheet

Author(s): [redacted] – Manger Property Asset

Document Title: Data Protection Impact Assessment - Project: Supply, Install and Maintain Public Space CCTV for Smart City/ Town Management

Review/Approval History

Date	Name	Position	Version Approved	Date Approved
07/01/2020	Data Protection Officer	n/a	1	07
20/08/2021	[redacted]	Manager Property Asset	1.1	20/08/2021
23/08/2021		Team Leader – Information Governance	1.1	23/08/2021

Version	Date	Brief Summary of Changes	Author
1.	January 2020	Final approved version	[redacted]
1.1	August 2021	Review carried out. Added in details on two new cameras installed in [redacted]. Revised position of one existing camera in [redacted]. [redacted] Added in Illegitimate Access risk	

Section 1 – Description of the Processing

What is the purpose of the processing? What is it intended to achieve? Who will benefit from the processing?
The images are held by Police Scotland for policing purposes. Other law enforcements agencies and security services may seek to access images through Police Scotland for similar purposes. The processing will result in: • Promotion of public safety • Crime prevention and detection • Reduction in criminal offences • Detecting anti-social behaviour • Prevention and protection of members of the public from violence and aggression • Other services as identified by Police Scotland Police Scotland and the general public will benefit from the more efficient policing of the areas covered by the cameras and reduction in the fear of crime. They will also assist in provision of evidence, protection of property, assistance in civil claims, assistance in public health and safety and emergency situations.
Who are the data subjects (e.g. customers, employees)?
The data subjects are members of the public.
Does the data include personal data concerning individuals other than the data subject? If so, list the groups affected (e.g. next of kin).
Data comprises: • Image of subject • Car registration • Property addresses depending on camera view available • Limited view into houses, restricted in accordance with Surveillance Camera Code of Practice (collateral intrusion). Privacy masks to the camera software will be applied in these situations to blank out direct views into houses.

What personal data will be processed? List personal identifiers, general categories of information, and any special categories as defined by the GDPR.	
List categories of information: Image of subject used to identify individuals involved in crime or for public safety. Vehicle Registration Numbers	Secondary images may be captured including: Health (disability) Political persuasion Ethnicity No special categories will be processed from the list above of available data.

How often will the processing typically occur in relation to an individual data subject? Is it part of a larger process? Provide an overview of the larger process.
The processing will occur on a daily basis and part of a larger process of ongoing monitoring of the CCTV feed by Police Scotland. The process will be the gathering and monitoring of the Open Space CCTV feed at a centralised monitoring station operated by Police Scotland. If an image/sound is required for evidentiary purposes it will be retained until the conclusion of the case. After this the recording will be deleted. The processing and retention of the data will be managed by Police Scotland in line with their Open Space CCTV data protection policy, codes of practice and compliance with the relevant legislation.

Describe each step of the processing. You should include what is done, who carries out each process step, and how the processing is done (e.g. paper record, computer system, photograph, etc.). An information processing flowchart may assist.		
What is done	By whom	How it is done
Data processing carried out by Police Scotland only.	Police Scotland	In line with Police Scotland's data protection policy and codes of practice.

How long will the information be stored? If it will be stored for a period after it is required for processing what is the basis for that retention period?
Information is not stored by Angus Council. Retention is in line with Police Scotland's policies and procedures. Recordings required for evidentiary purposes will be retained until closure of the case. It is not possible to specify an exact time limit.

What systems (electronic or paper based) will be used to store and process the data? Include descriptions of the hardware, software, paper filing systems, etc.

The system proposed is the [redacted] System which includes [redacted] video surveillance management software. This system gives an increased level of situational awareness, allowing greater collaboration both within organisations and with emergency response teams.

The system also has the ability to extract data sets for use within the Open Data Platform.

Data is saved [redacted]

There are [redacted] cameras across seven Angus burghs as part of the overall system, the cameras include tilt, pan and zoom functions together with selects ANPR options. Any replacement cameras installed will be in the same positions and provide the same functionality as the existing cameras. The cameras are placed within the town limits of Arbroath, Brechin, Carnoustie, Forfar, Kirriemuir, Monifieth and Montrose.

[redacted]

Who will have access to the personal data during processing? List the staff roles and the legitimate reasons for access.

Angus Council have no access to this information. Details contained in Police Scotland's policies and procedures as the main data controller and processor.

Will the data be shared with third parties? If so, list the parties and any limits to the range of personal information which will be shared.

Third Party Recipient	Limitations to Information Shared
Police Scotland	Polices Scotland manage, process and record images and sound from the Open Space CCTV cameras throughout Angus.

Section 2 – Proportionality and Necessity of the Processing

What measures have been taken to ensure the processing will be specific, explicit and legitimate?
The equipment will only be used by trained operatives employed by Police Scotland and/or the Scottish Police Authority. The equipment will be set up in line with the Surveillance Camera Code of Practice and Police Scotland's policies and procedures for CCTV systems.
On what legal basis or bases is the data to be processed?
The processing satisfies Data Protection Act 2018 conditions 5(d) of schedule 2 – the processing is necessary for the exercise of any other functions of a public nature in the public interest. The processing satisfies Article 6(1) (e) of the General Data Protection Regulation – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The processing satisfies section 33(2)(b) of the Data Protection Act 2018– the processing of personal data for any of the law enforcement purposes is lawful only if and to the extent it is based on law and the processing it necessary for the performance of a task carried out for that purpose by a competent authority.

If the rights of data subjects eg *right to be informed, right of erasure, right of access, right of rectification* etc (see section 3 below) are restricted by the legal basis for processing, what reasons are there for considering the processing to be proportionate?
The rights of the data subjects are restricted in line with the processing requirements. This is proportionate as the processing is in pursuance of a public task/authority relating to law enforcement under Police Scotland's duties.
What reasons are there for considering the processing is necessary to achieve the stated purpose and that there are no other reasonable ways to achieve that purpose?
The recorded images will be used for crime prevention /detection and the use of CCTV is the minimum required for gathering images in a reasonable and proportionate operation. This removes the need for corroboration, removes ambiguity and provides quality, accurate evidence.
What measures have been taken to ensure the personal information collected is both adequate to achieve the purpose of the processing and limited to on that information which is necessary to achieve the purpose?
Camera positions are based in line the requirements of Police Scotland to achieve the necessary level of policing required in the identified areas. Police Scotland will use their crime and public order statistics to identify these areas. All images are subject to restrictions on the period of time they can be retained in line with Police Scotland's policies and procedures.
What measures have been taken to ensure the information is accurate and is kept up to date?
This is not relevant to recorded CCTV data as the images have no requirement to be updated.

Section 3 – Protecting Data Subject Rights

How will the right of the subject to be informed be met?
Signage at the CCTV camera sites and in line with Police Scotland's published privacy notices.
If data subjects retain a right of **access** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Rights to access the data will be in line with Police Scotland's policies and procedures and in accordance with the right to a Subject Access Request under the General Data Protection Regulation.
If data subjects retain a right to **rectification** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable

If data subjects retain a right to **erasure** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Rights to erase the data will be in line with Police Scotland's policies and procedures.
If data subjects retain a right to **data portability** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If data subjects retain a right to **restrict processing** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
No applicable.

If data subjects retain a right to **object** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If some of the processing will be carried out by third party data processors, are there adequate contracts or service level agreements in place specifying the requirements for the processes undertaken, data sharing limitations, security requirements, and duties in relation to data subjects' rights? What arrangements are in place for monitoring compliance and reporting breaches?
Police Scotland are the data controllers and main data processors of the data. Angus Council only provides the hardware to allow the data to be passed on with no intervention in the data feed. All compliance requirements are in line with Police Scotland's policies and procedures.
Is the personal data held and processed only within the UK or the European Economic Area? If not, what safeguards are in place to ensure the security, integrity and confidentiality of the data?
The data is held and processed within the UK.
If the processing covered by this DPIA is considered to pose a high risk in the absence of mitigation, has there been prior consultation with the Information Commissioner? What was the outcome of that consultation?
The information referred to in this DPIA is deemed high risk in line with 35(3)(c): "a systematic monitoring of a publicly accessible area on a large scale". The DPIA may require to be referred to the ICO for joint consultation along with Dundee City Council, Perth & Kinross Council and Police Scotland.

Section 4 – Data Protection Risk Assessment

Use this section to identify the risks to the rights and freedoms of data subjects posed by the processing covered in this DPIA.

There are four main sources of risk which need to be considered:

- Illegitimate access to data
- Undesired modification of data
- Disappearance or destruction of data
- Inappropriate or uncontrolled sharing of data

For each of these categories, identify where in the processing the risk of a breach might arise and how it might arise. For each risk you need to quantify the:

- Likelihood of a breach occurring
  (1=negligible, 2=low, 3=moderate, 4=high, 5=extremely likely)
- The severity of the impact of a breach on the data subjects rights and freedoms
  (1=negligible, 2=minor, 3=moderate, 4=major, 5=catastrophic)
- The overall risk score (likelihood multiplied by severity)

You should then list the actions you will take to mitigate or eliminate each risk. The aim is to demonstrate that you have designed the process in such a way as to prevent or minimise the risk of a breach occurring.

If the overall score for any risk is 15 or more then you must seek prior consultation with the Data Protection Officer before implementing the processing covered by this DPIA.

Add rows to the tables as necessary.

1.1 Illegitimate Access

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Angus Council do not have access or process the data so risk as not applicable	1	1	1	Any risks identified with regard to the data will be considered by Police Scotland as the data controller and processer as part of their policies and procedures for operating the system

1.2 Undesired Modification

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Not applicable.				

1.3 Disappearance or Destruction

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Not applicable.				

1.4 Inappropriate or uncontrolled sharing

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Not applicable.				

Section 5 – Data Protection Officer's Advice

I am satisfied that there are no data issues in relation to CCTV cameras being placed in various sites across Angus.

Police Scotland are the data controllers and main data processors of the data. Angus Council only provides the hardware to allow the data to be passed on with no intervention in the data feed.

I am satisfied that no personal data is being stored by Angus Council who are providing equipment only. All images will be owned, viewed and managed by Police Scotland.

Signage at the CCTV camera sites will be in line with Police Scotland's published privacy notices.

Final decision if Data Controller's advice is contrary to the proposed processing

Section 6 – Outcome of Consultation with Data Subjects (if applicable)

DATA PROTECTION IMPACT ASSESSMENT

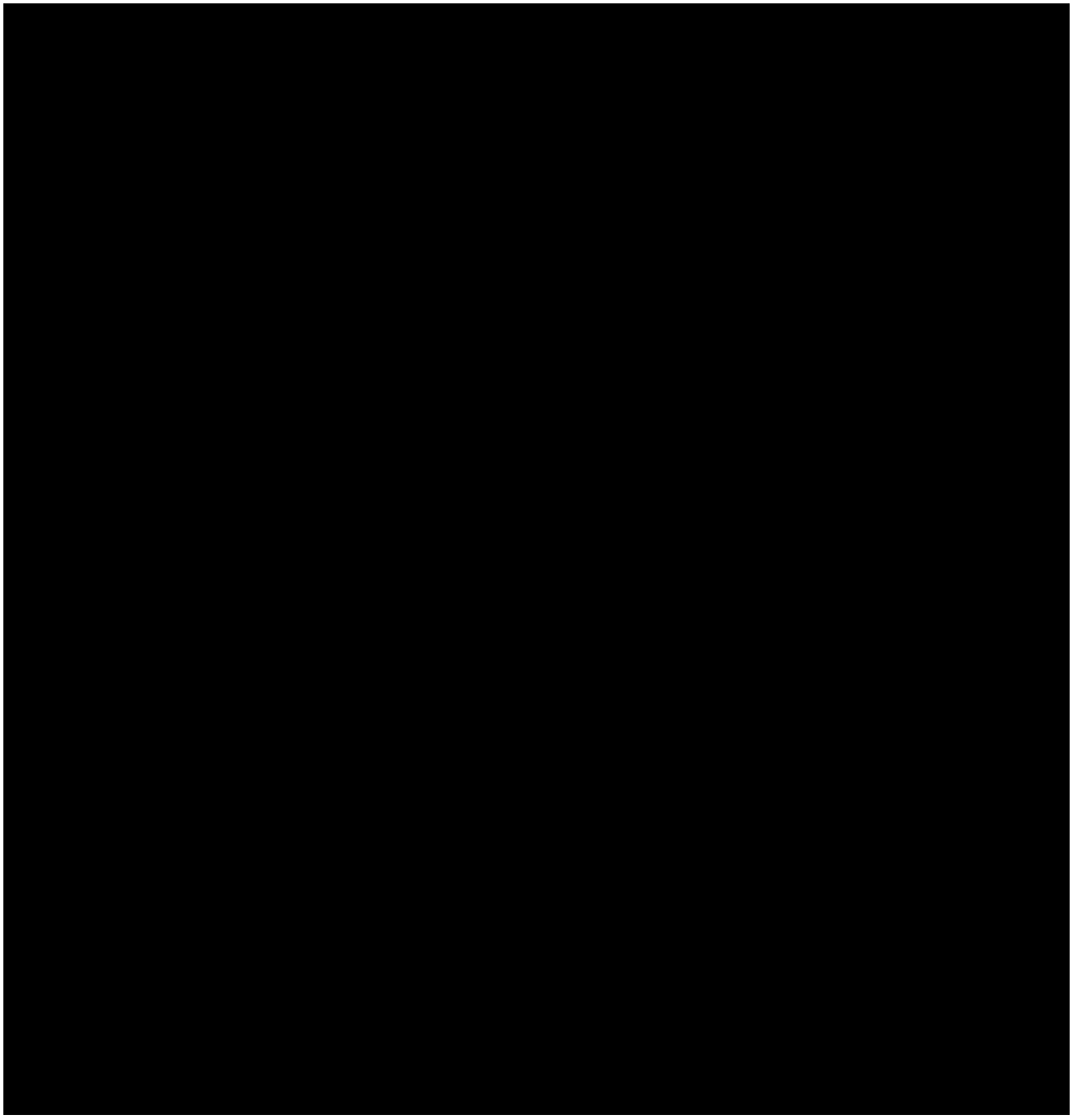
ANNEX 1 – PUBLIC SPACE CCTV CAMERA POSITION DETAILS

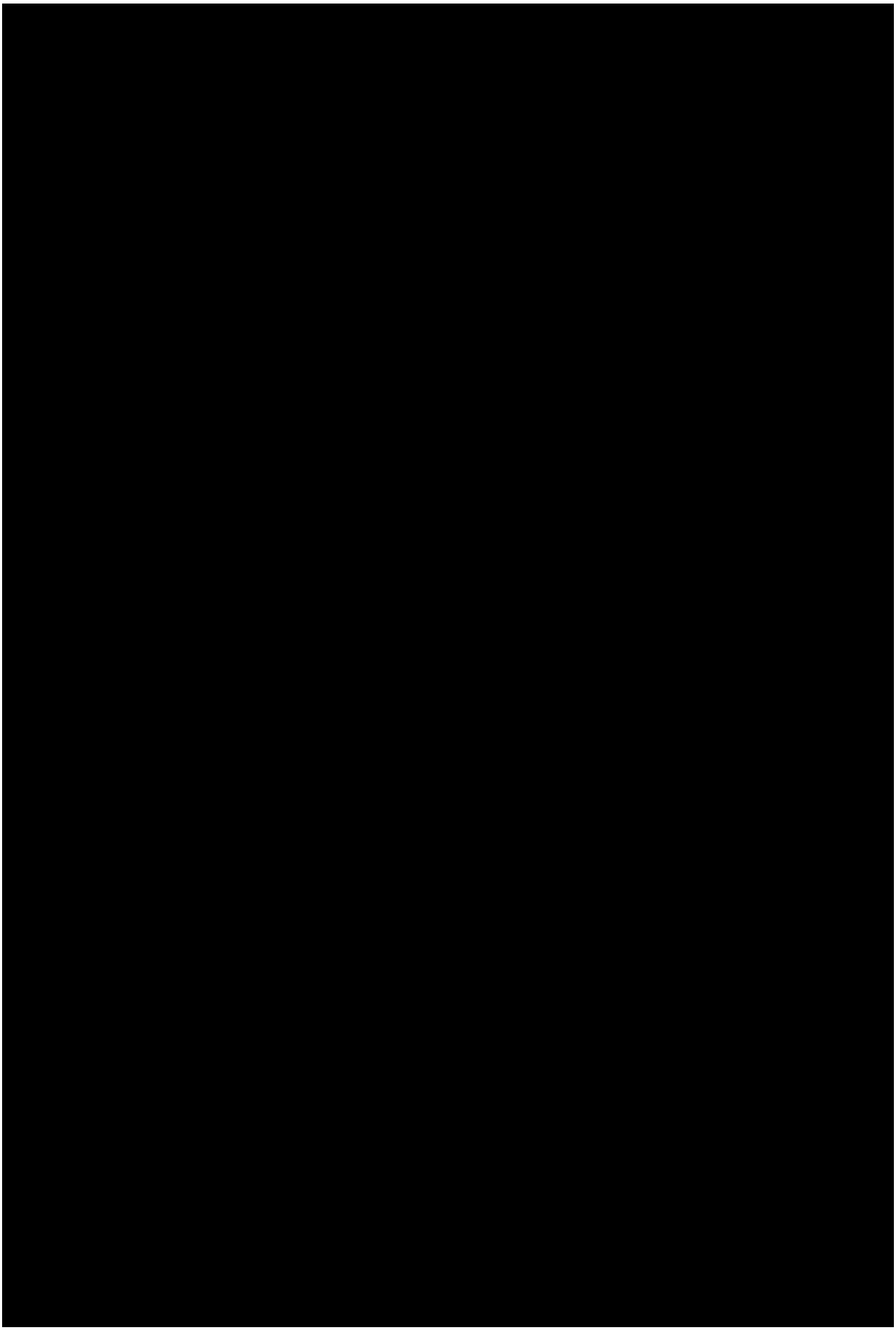
Project	CCTV for Smart City/ Town Management - ANGUS
Camera Number (if known)	[redacted]
Camera location	[redacted]
Camera type	Bosch [redacted]
Analytic functionality	None
Connection type	[redacted]
Transmission protection	[redacted]

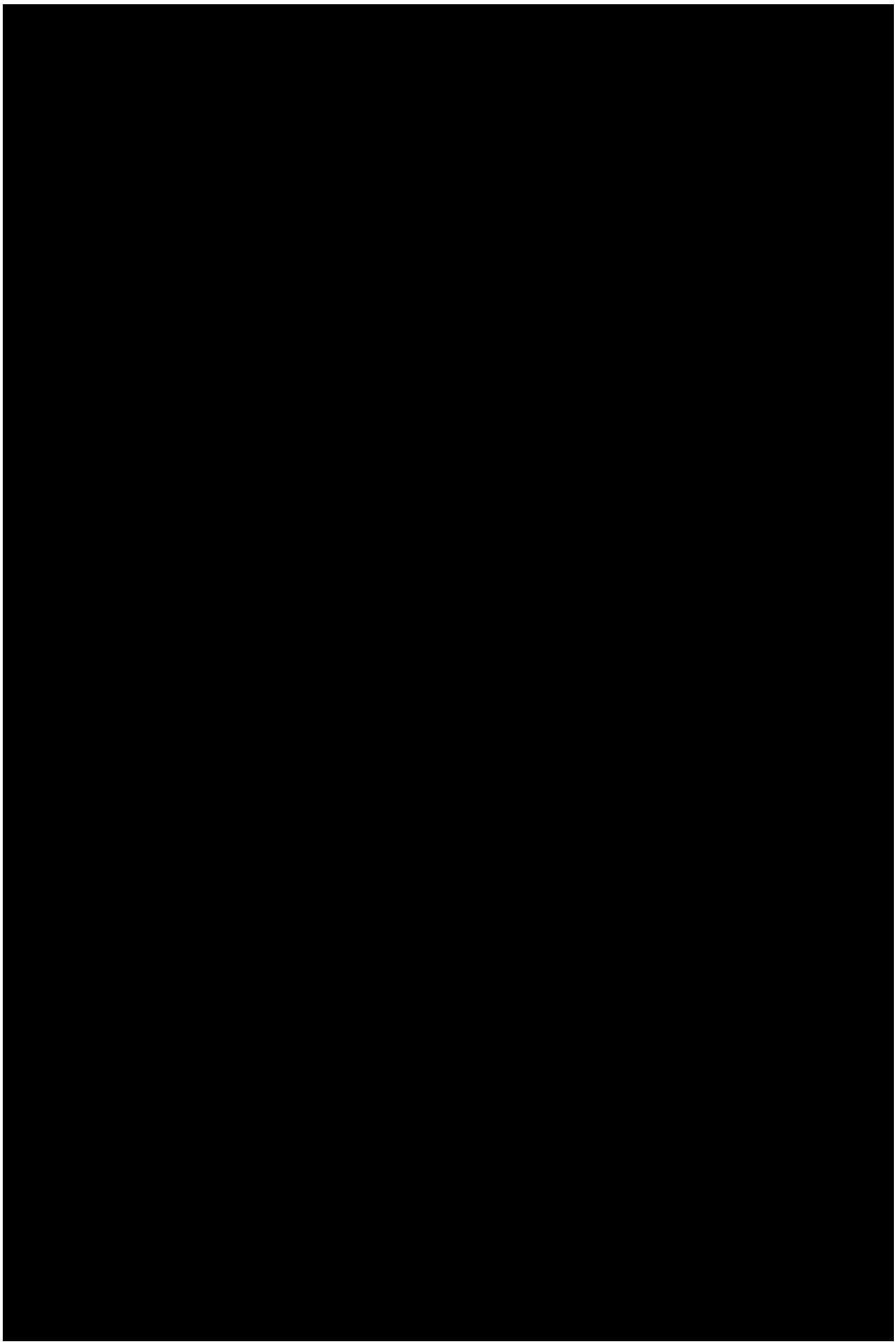
Purpose of this camera	Crime Detection Crime Prevention Public Safety

Other information	Cameras are a mixture of wall bracket and pole mounted as noted below.

CAMERA LOCATION ADDRESSES







Data Protection

Data Protection Impact Assessment

Project: Use of Vehicle Camera Monitoring System with Remote Access

Environmental Services

"Privacy by Design"
Office of the Information Commissioner

Data Protection Impact Assessment

Name or Description of Process

Use of vehicle camera monitoring system with remote access

Date Assessment Approved	**Review Date**
30 September 2021	30 September 2022

Approvals	**Signatures**	
Senior Responsible Manager	[redacted]	
Process Owner		
Data Protection Officer		

Section 1 – Description of the Processing

What is the purpose of the processing? What is it intended to achieve? Who will benefit from the processing?
The ability to view and review footage captured at the time and location of alleged incidents will allow us to provide evidence in the case of a false insurance claim, or conversely to recognise our liability in cases of false statements by operatives. Overall, access to an accurate and impartial record of accidents will allow insurance claims to be resolved fairly, whether false or otherwise. The live and recorded footage allows us to accurately identify drivers and operatives who may require assessment following repeated accidents, rather than relying solely on staff reporting or admitting to incidents. Live and recorded footage can be used to monitor staff practises by random spot checks to demonstrate a proactive approach to duty of care and staff wellbeing. Should footage reveal a serious concern, it could result in using downloaded footage as part of any disciplinary action. The presence of the camera system protects our employees from violence and aggression whilst carrying out their duties at work and allows us to provide evidence to Police Scotland if situations escalate. Remote access to the vehicle footage will allow authorised users to promptly investigate customer complaints such as missed bins without the delay of waiting on access and time required to interrogate the recorded footage on the hard drive. Without removing the hard drive to view footage means the vehicle can carry on with its duties with the CCTV system still recording and in operation.
Who are the data subjects (e.g. customers, employees)?
Employees and members of the public
Does the data include personal data concerning individuals other than the data subject? If so, list the groups affected (e.g. next of kin).
Visible vehicle registrations
What personal data will be processed? List personal identifiers, general categories of information, and any special categories as defined by the GDPR.

Image of subject used to identify individuals involved in crime or for public safety. Vehicle Registration Numbers	Secondary images may be captured including: Health (disability) Ethnicity

How often will the processing typically occur in relation to an individual data subject? Is it part of a larger process? Provide an overview of the larger process.

The system will store around 150 hours of footage and then automatically overwritten.

Footage required for evidentiary purposes will be marked/downloaded as such in order that they are not part of the software's automatic deletion programme.

If an image is required for evidentiary purposes it will be retained until the conclusion of the case (this includes requirement to retain in event of appeal and/or associated legal claim). After this the recording will be deleted.

Footage will only be reviewed upon a report of an incident requiring review or evidence capture. There is a separate policy document on the proper use of vehicle camera monitoring system.

Describe each step of the processing. You should include what is done, who carries out each process step, and how the processing is done (e.g. paper record, computer system, photograph, etc.). An information processing flowchart may assist.

What is done	By whom	How it is done
Image is recorded	CCTV cameras	Cameras continuously record/ stream whilst ignition is on
Incident or event reported	Employee or member of the public	Employee to line manager. Member of the public to council through Accessline
Footage (live or recorded) reviewed on Council issued PC/ laptop	Management Team/ Authorised person	Log online to camera system
Footage not required for evidence is left on system	CCTV system	Footage automatically overwritten after approx. 150 hours of further footage stored

Footage required for evidence.	Management Team/ Authorised person	[redacted]
Footage for completed investigations	Manager/ Authorised person	Manually deleted once case is closed (taking into account any possible appeal or claim)
Footage may be passed to third parties (e.g. releasing footage to our insurance company in support of a motor claim form).	Manager/ Authorised person	[redacted]
Request from data subject to view footage.	Manager/ Authorised person	Data subject attends council office to review footage
Footage utilised for staff training purposes.	Manager/ Authorised person	Footage is played to employee to demonstrate examples of good/ bad practice thereafter deleted
Footage utilised for disciplinary purposes – would include sharing with HR and others included in the process (e.g. union rep).	Manager/ Authorised person	Footage is played to employee and those involved in the investigation at a council premises by an authorised person.

How long will the information be stored? If it will be stored for a period after it is required for processing what is the basis for that retention period?
Footage will automatically be overwritten after 150 hours has been stored. Downloaded footage required for evidentiary purposes will be retained until closure of the case. It is not possible to specify an exact time limit
What systems (electronic or paper based) will be used to store and process the data? Include descriptions of the hardware, software, paper filing systems, etc.
Client based software online to view and download footage. Any footage that requires to be kept [redacted] with limited access from Waste Services Management only.
Who will have access to the personal data during processing? List the staff roles and the legitimate reasons for access.
Waste Operations – Team Leader (x1), Operations Assistant managers (x2) and Transport and Technical Co-ordinator (x1) - reviewing footage and determining the need for downloading for evidentiary purposes, passing to third parties or for training purposes. Angus Council employees as required in disciplinary proceedings and any other third party involved as outlined in the disciplinary process.
Will the data be shared with third parties? If so, list the parties and any limits to the range of personal information which will be shared.

Third Party Recipient	Limitations to Information Shared
Police Scotland- Procurator Fiscal	[redacted]
Insurance Company	

	Footage and personal details of only those involved in the insurance claim - [redacted]

Section 2 – Proportionality and Necessity of the Processing

What measures have been taken to ensure the processing will be specific, explicit and legitimate?
To protect the privacy of the employees, system users will follow the 'CCTV [redacted] Cameras Procedure'.
On what legal basis or bases is the data to be processed?
To assist with compliance of the following: • Health & Safety at Work etc Act 1974 • Section 172 of the Road Traffic Act 1988 • Para 10 of Schedule 1 Data Protection Act 2018 (protection, detection of unlawful acts)
If the rights of data subjects eg *right to be informed, right of erasure, right of access, right of rectification* etc (see section 3 below) are restricted by the legal basis for processing, what reasons are there for considering the processing to be proportionate?
Processing is proportionate in relation to providing accurate information for third parties in cases such as insurance claims, fraudulent insurance claims and matters involving Police Scotland such as motor accidents or violence and aggression towards our employees. Signage is in place on vehicles fitted with CCTV cameras to make people aware of the system in place.

What reasons are there for considering the processing is necessary to achieve the stated purpose and that there are no other reasonable ways to achieve that purpose?
Other than initial the recording, further processing of the recorded footage is only carried out when an allegation is made by either an employee or a member of the public. The recorded footage from the system provides accurate evidence. In most cases there would be no other camera footage or independent witness statements available to verify accuracy of a report.
What measures have been taken to ensure the personal information collected is both adequate to achieve the purpose of the processing and limited to on that information which is necessary to achieve the purpose?
Footage is reviewed only when an incident has been reported. Recorded footage is only downloaded when it is appropriate for using as evidence for third party, using during disciplinary matters or for training purposes.
What measures have been taken to ensure the information is accurate and is kept up to date?
All images are time and date stamped. Camera system equipment is maintained.

Section 3 – Protecting Data Subject Rights

How will the right of the subject to be informed be met?

Signage on the exterior of the vehicle.
If data subjects retain a right of **access** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Within 40 calendar days, the data subject will be required to submit a request to view the data, which can be done either verbally to their line manager or by writing to a system administrator or senior manager. Members of the public will be required to submit a request to view the footage via ACCESSline. All requests will be considered having regard to the rights and interests of all data subjects concerned.
If data subjects retain a right to **rectification** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable
If data subjects retain a right to **erasure** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Would be considered only if the footage is not required for evidential purposes and having regard to the rights and interests of all data subjects and the public interest.
If data subjects retain a right to **data portability** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?

Not applicable
If data subjects retain a right to **restrict processing** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Any requests would be considered having regard to the rights and interests of all data subjects and the public interest.
If data subjects retain a right to **object** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Any requests would be considered having regard to the rights and interests of all data subjects and the public interest.
If some of the processing will be carried out by third party data processors, are there adequate contracts or service level agreements in place specifying the requirements for the processes undertaken, data sharing limitations, security requirements, and duties in relation to data subjects' rights? What arrangements are in place for monitoring compliance and reporting breaches?
Angus Council has a data protection policy in place and a data breach reporting process. [any third party contracts to be reviewed for DP compliance wording]

Is the personal data held and processed only within the UK or the European Economic Area? If not, what safeguards are in place to ensure the security, integrity and confidentiality of the data?
Data is stored in the UK only.
If the processing covered by this DPIA is considered to pose a high risk in the absence of mitigation, has there been prior consultation with the Information Commissioner? What was the outcome of that consultation?
Not applicable.

Section 4 – Data Protection Risk Assessment

Use this section to identify the risks to the rights and freedoms of data subjects posed by the processing covered in this DPIA.

There are four main sources of risk which need to be considered:

- Illegitimate access to data
- Undesired modification of data
- Disappearance or destruction of data
- Inappropriate or uncontrolled sharing of data

For each of these categories, identify where in the processing the risk of a breach might arise and how it might arise. For each risk you need to quantify the:

- Likelihood of a breach occurring
  (1=negligible, 2=low, 3=moderate, 4=high, 5=extremely likely)
- The severity of the impact of a breach on the data subjects rights and freedoms
  (1=negligible, 2=minor, 3=moderate, 4=major, 5=catastrophic)
- The overall risk score (likelihood multiplied by severity)

You should then list the actions you will take to mitigate or eliminate each risk. The aim is to demonstrate that you have designed the process in such a way as to prevent or minimise the risk of a breach occurring.

If the overall score for any risk is 15 or more then you must seek prior consultation with the Data Protection Officer before implementing the processing covered by this DPIA.

Add rows to the tables as necessary.

1.1 Illegitimate Access

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Data is accessible and accessed by employees	2	2	4	Access is only available to authorised persons who have access to Angus Council restricted folders on network
[redacted]	1	2	2	[redacted]

1.2 Undesired Modification

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Data is modified incorrectly by employees	1	1	1	Software does not allow users to modify data

1.3 Disappearance or Destruction

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Footage is deleted in error	2	2	4	[redacted]
Footage is deleted intentionally	2	2	4	[redacted]

1.4 Inappropriate or uncontrolled sharing

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Employee shares information without permission	1	2	2	Access is only available to employees who have undertaken Angus Council data protection training. Only authorised persons to view footage.

Section 5 – Data Protection Officer's Advice

Having regard to the interest of AC employees, third parties, the council and the public interest, I agree that the proposals are acceptable, subject to compliance and review of third party contractor agreement (if any).

[redacted]

30 September 2021

Final decision if Data Controller's advice is contrary to the proposed processing

Section 6 – Outcome of Consultation with Data Subjects (if applicable)

Data Protection

Data Protection Impact Assessment

Project: Blackfriars Court CCTV

"Privacy by Design"
Office of the Information Commissioner

Data Protection Impact Assessment

Name or Description of Process

Installation of CCTV in Blackfriars Court (Retirement Housing)

Date Assessment Approved	Review Date

Approvals	Signatures	
Senior Responsible Manager	[redacted]	
Process Owner		
Data Protection Officer		

Section 1 – Description of the Processing

What is the purpose of the processing? What is it intended to achieve? Who will benefit from the processing?
The purpose of the processing is to install CCTV at Blackfriars Court. It is intended to achieve better security after numerous break ins and a lot of cold callers over the last few months [redacted] The residents of Blackfriars Court will mostly benefit from the processing, as well as Housing staff. The police may also benefit from the installation of CCTV at Blackfriars Court. The processing will result in: · Promotion of public safety · Crime prevention and detection · Reduction in criminal offences · Detecting anti-social behaviour · Prevention and protection of members of the public from violence and aggression · Other services as identified by Police Scotland.
Who are the data subjects (e.g. customers, employees)?
The data subjects here would mainly be the residents but could also include visitors, workmen, council employees etc.
Does the data include personal data concerning individuals other than the data subject? If so, list the groups affected (e.g. next of kin).
The data includes recorded footage and this would be covering anyone entering Blackfriars Court so this will not only impact residents but also any visitors (personal visitors and any non-resident). Data comprises: • Image of subject • Property addresses depending on camera view available • Limited view into houses, restricted in accordance with Surveillance Camera • Code of Practice (collateral intrusion).

What personal data will be processed? List personal identifiers, general categories of information, and any special categories as defined by the GDPR.	
List categories of information: Images of subjects used to identify individuals involved in crime or for public safety. Audio (although this functionality is available, it will be turned off).	Secondary images may be captured including: Health (disability) Ethnicity No special categories will be processed from the list above of available data

How often will the processing typically occur in relation to an individual data subject? Is it part of a larger process? Provide an overview of the larger process.
Video recordings will be captured in real time and stored for a two-week period before being recorded over. These recordings will not be viewed unless there is a crime/disturbance in which case this footage may be handed over to Police Scotland who would then become the data controller of the footage. After the police have been provided with the relevant information, the video recording would be recorded over.

Describe each step of the processing. You should include what is done, who carries out each process step, and how the processing is done (e.g. paper record, computer system, photograph, etc.). An information processing flowchart may assist.		
What is done	By whom	How it is done
Video recording	[redacted]	CCTV

How long will the information be stored? If it will be stored for a period after it is required for processing what is the basis for that retention period?
Information will be stored for two weeks at a time then recorded over automatically (no human intervention). The information is not stored by Angus Council [redacted] (for the purposes of this DPIA will be known as the hard drive) [redacted]

This data can only be accessed by the police or the Council appointed authorised responsible person [redacted]. The recordings are recorded over after a two week period and there are no other devices involved

What systems (electronic or paper based) will be used to store and process the data? Include descriptions of the hardware, software, paper filing systems, etc.

The footage will be stored on [redacted]

Who will have access to the personal data during processing? List the staff roles and the legitimate reasons for access.

The people who will have access will include Housing staff [redacted] but the police can also have access should an incident occur. [redacted]

No external individual can access the information [redacted] This feature is there to allow only permitted authorised personnel to access the data stored.

Will the data be shared with third parties? If so, list the parties and any limits to the range of personal information which will be shared.

Third Party Recipient	Limitations to Information Shared
Police Scotland	Police Scotland will only have access to this if a crime has been reported.

Section 2 – Proportionality and Necessity of the Processing

What measures have been taken to ensure the processing will be specific, explicit and legitimate?
The equipment will only be used by Angus Council Housing but images may potentially be shared with Police Scotland in relation to any crimes The equipment will be set up [redacted]
On what legal basis or bases is the data to be processed?
Legitimate interests – article 6(1)(f). Processing is necessary for security aspects of Blackfriars Court Data Protection Act 2018 requires that any surveillance must only be used in pursuit of one or more legitimate (reasonable, lawful and appropriate) purposes and be necessary, proportionate and fair to meet an identified and pressing need. The installation of CCTV is considered as lawful, fair and proportionate
If the rights of data subjects eg *right to be informed, right of erasure, right of access, right of rectification* etc (see section 3 below) are restricted by the legal basis for processing, what reasons are there for considering the processing to be proportionate?
The information is only stored for two weeks at a time and then deleted automatically. This CCTV is not monitored daily and will only be viewed when required. The recorded images may be used for crime prevention /detection and the use of CCTV is the minimum required for gathering images in a reasonable and proportionate operation. This removes the need for corroboration, removes ambiguity and provides quality, accurate evidence. If a crime is recorded and the Police require a copy, they will be provided a copy and they then become the Data Controllers of that copy. As per the above, our copy of the footage will be recorded over in two weeks' time.
What reasons are there for considering the processing is necessary to achieve the stated purpose and that there are no other reasonable ways to achieve that purpose?
The purpose of processing is necessary for security reasons [redacted]

What measures have been taken to ensure the personal information collected is both adequate to achieve the purpose of the processing and limited to on that information which is necessary to achieve the purpose?
Camera positions [redacted] The images are only stored for two weeks at a time and not held any longer. All tenants of Blackfriars Court have signed documentation agreeing to the use of CCTV as they feel that this is a preventive measure there to help safeguard them against continual cold calling/fraudulent activity.
What measures have been taken to ensure the information is accurate and is kept up to date?
This is not relevant to recorded CCTV data as the images have no requirement to be updated.

Section 3 – Protecting Data Subject Rights

How will the right of the subject to be informed be met?
Signage at the CCTV camera sites will be displayed so that people know that they are in operation. All tenants of Blackfriars Court have signed documentation agreeing to the use of CCTV.
If data subjects retain a right of **access** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
People will have access to this information and can access this by requesting through a Subject Access Request as long as it is within the 2 week period of this being held.
If data subjects retain a right to **rectification** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?

N/A as it is an image
If data subjects retain a right to **erasure** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
N/A - however, these recordings are automatically overwritten after 14 days.
If data subjects retain a right to **data portability** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
N/A
If data subjects retain a right to **restrict processing** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
N/A
If data subjects retain a right to **object** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
N/A. All new tenants will be asked to agree to the CCTV as it will be included in their tenancy agreement upon signup.
If some of the processing will be carried out by third party data processors, are there adequate contracts or service level agreements in place specifying the requirements for the processes undertaken, data sharing limitations, security requirements, and duties in relation to data subjects' rights? What arrangements are in place for monitoring compliance and reporting breaches?
Although data breaches are unlikely, they would be treated the same way as any other data breaches are.

Is the personal data held and processed only within the UK or the European Economic Area? If not, what safeguards are in place to ensure the security, integrity and confidentiality of the data?
The data is held and processed with the UK.
If the processing covered by this DPIA is considered to pose a high risk in the absence of mitigation, has there been prior consultation with the Information Commissioner? What was the outcome of that consultation?
The information referred to in this DPIA does not require consultation with the Information Commissioner.

Section 4 – Data Protection Risk Assessment

Use this section to identify the risks to the rights and freedoms of data subjects posed by the processing covered in this DPIA.

There are four main sources of risk which need to be considered:

- Illegitimate access to data
- Undesired modification of data
- Disappearance or destruction of data
- Inappropriate or uncontrolled sharing of data

For each of these categories, identify where in the processing the risk of a breach might arise and how it might arise. For each risk you need to quantify the:

- Likelihood of a breach occurring
  (1=negligible, 2=low, 3=moderate, 4=high, 5=extremely likely)
- The severity of the impact of a breach on the data subjects rights and freedoms
  (1=negligible, 2=minor, 3=moderate, 4=major, 5=catastrophic)
- The overall risk score (likelihood multiplied by severity)

You should then list the actions you will take to mitigate or eliminate each risk. The aim is to demonstrate that you have designed the process in such a way as to prevent or minimise the risk of a breach occurring.

If the overall score for any risk is 15 or more then you must seek prior consultation with the Data Protection Officer before implementing the processing covered by this DPIA.

Add rows to the tables as necessary.

1.1 Illegitimate Access

Risk Description	Likelihood	Severity	Score	Mitigation Actions
The CCT [redacted]	1	1	1	[redacted] the risk of illegitimate access is low.

1.2 Undesired Modification

Risk Description	Likelihood	Severity	Score	Mitigation Actions
N/A				

1.3 Disappearance or Destruction

Risk Description	Likelihood	Severity	Score	Mitigation Actions
N/A				

1.4 Inappropriate or uncontrolled sharing

Risk Description	Likelihood	Severity	Score	Mitigation Actions
N/A				

Section 5 – IT advice

If the DPIA relates to a new system or app IT advice is required to be noted here:

(This requires to be completed before passing to the DPO for comments)

Section 6 – Data Protection Officer's Advice

I note that this equipment (cameras or hard drive) will not be owned or maintained by Angus Council. [redacted]

All residents have signed an agreement to say they consent for the CCTV to be erected and this permission is being held by the housing service. All new residents will be advised and also asked to consent.

Signs will be erected so that residents, visitors etc to the complex are aware that CCTV is in operation.

Audio will be switched off to respect the privacy of those people living and visiting the complex

No computer is involved or any hardware that belongs to Angus Council.

[redacted]

[redacted]

Angus Council employees will only access the data if an incident is reported to them and will only share with Police Scotland if a crime is reported and it is felt that information from the CCTV will assist with a conviction.

There is no need for further council involvement other than to make sure all aspects of data security and privacy of the residents and visitors has been taken into account.

Final decision if Data Controller's advice is contrary to the proposed processing

Section 7 – Outcome of Consultation with Data Subjects (if applicable)

Data Protection

Data Protection Impact Assessment

Project: Installation and use of fixed CCTV cameras to Public Toilets at Forfar Loch Country Park

"Privacy by Design"
Office of the Information Commissioner

Data Protection Impact Assessment

Name or Description of Process

Installation and maintenance of a fixed external CCTV System to Public Toilets at Forfar Loch Country Park.

Date Assessment Approved	Review Date

Approvals	Signatures
Senior Responsible Manager	Ian Cochrane - Director of Infrastructure Angus Council
Process Owner	System, Data Controller & Processor: [redacted] - Team Leader Property Maintenance, Angus Council Processor: [redacted] - Senior Manager (Sports & Leisure) ANGUSalive
Data Protection Officer	[redacted] - Service Leader Legal & Democratic

Amendment Form

Version	Date	Brief Summary of Changes	Author
Version 2	13/05/2022	ANGUSalive staff added to allow access to data	[redacted]

Section 1 – Description of the Processing

What is the purpose of the processing? What is it intended to achieve? Who will benefit from the processing?
The images are held by Angus Council for public safety and detecting criminal and anti-social behaviour. Images may be accessed by Police Scotland for law enforcement purposes. The processing will result in: • Promotion of public safety • Crime prevention and detection • Reduction in criminal offences • Detecting anti-social behaviour The public will benefit from the reduction in crime and associated fear of crime. It will also assist in provision of evidence, protection of property, assistance in civil claims, assistance in public health and safety.
Who are the data subjects (e.g. customers, employees)?
The data subjects are members of the public/service users.
Does the data include personal data concerning individuals other than the data subject? If so, list the groups affected (e.g. next of kin).
The data doesn't include personal data concerning any other individuals and will only record images of the subject.
What personal data will be processed? List personal identifiers, general categories of information, and any special categories as defined by the GDPR.

List categories of information:	Secondary images may be captured including:
Image of subject used to identify individuals involved in crime, anti-social behaviour or for public safety.	Health (disability) Political persuasion Ethnicity

How often will the processing typically occur in relation to an individual data subject? Is it part of a larger process? Provide an overview of the larger process.

The processing will occur on a daily basis as the CCTV will be recording 24 hours a day. If an image is required for evidentiary purposes, it will be retained until the conclusion of the case. After this the recording will be deleted.

Recordings not required for evidentiary purposes are automatically deleted within 30 days. Those recordings required for evidentiary purposes require to be marked as such in order that they are not part of the software's automatic deletion programme.

Describe each step of the processing. You should include what is done, who carries out each process step, and how the processing is done (e.g. paper record, computer system, photograph, etc.). An information processing flowchart may assist.		
What is done	By whom	How it is done
Images only is recorded.	Automatic recording [redacted]	Recording automatically operates on a 24-hour basis
If notification received from ANGUSalive/Angus Council staff or by a third party of an incident recordings are reviewed.	Recordings are only accessed by Property Assets Maintenance Team Clerk of Works or by ANGUSalive Countryside Rangers staff and their line management.	[redacted]
Once reviewed relevant images are saved for retention	Staff as noted above.	Automatically
Recordings not marked for retention are deleted	Software	Automatically
Recordings marked for retention are deleted	Staff as noted above.	Manually once case closed or no further action is taken.
Recording may be passed to Police Scotland or other third party (e.g., criminal activity, anti-social behaviour may be shared).	Staff as noted above	[redacted]
Signs will be installed on the building in accordance with guidance.	Installation contractor. Checked by Property Assets Maintenance Team Clerks of Works.	Signage securely fixed to buildings.

How long will the information be stored? If it will be stored for a period after it is required for processing what is the basis for that retention period?

Information will automatically be deleted after 30 days unless specifically marked for retention.

Recordings required for evidentiary purposes will be retained until closure of the case. It is not possible to specify an exact time limit.

What systems (electronic or paper based) will be used to store and process the data? Include descriptions of the hardware, software, paper filing systems, etc.

The system proposed comprises:

- Dahua [redacted]
- Dahua [redacted]
- [redacted]

Appropriate software will be used to manged and operate the system [redacted]

The cameras will be mounted externally on the toilet extension and ANGUSalive Countryside Rangers Base at Forfar Loch Country Park to cover the exterior of the buildings.

Who will have access to the personal data during processing? List the staff roles and the legitimate reasons for access.

Property Asset Maintenance Team Clerks of Works and ANGUSalive Countryside Rangers - reviewing footage and determining the need for retention following an incident. Footage may also be reviewed by Clerk of Works and Countryside Rangers line management if requested. [redacted]

Downloading of data for use by Police Scotland.

Police Scotland – receipt of footage [redacted]

Will the data be shared with third parties? If so, list the parties and any limits to the range of personal information which will be shared.	
Third Party Recipient	Limitations to Information Shared
Police Scotland	Criminal proceedings – footage for evidence [redacted]

Section 2 – Proportionality and Necessity of the Processing

What measures have been taken to ensure the processing will be specific, explicit and legitimate?
The data will only be accessed following an incident either internally or externally at the toilets which has been identified by the ANGUSalive Countryside Rangers and/or reported to the Property Assets Maintenance team. The Property Assets Maintenance team and ANGUSalive Countryside Rangers will have access to the data [redacted] The CCTV will be fixed externally and aimed at specific areas. The angle and area covered will be considered to limit intrusion into other areas. Appropriate signage will be in place.
On what legal basis or bases is the data to be processed?

The processing satisfies Data Protection Act 2018 conditions 5(d) of schedule 2 – the processing is necessary for the exercise of any other functions of a public nature in the public interest.

The processing satisfies Article 6(1) (e) of the General Data Protection Regulation – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The processing satisfies section 33(2)(b) of the Data Protection Act 2018– the processing of personal data for any of the law enforcement purposes is lawful only if and to the extent it is based on law and the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

If the rights of data subjects eg *right to be informed, right of erasure, right of access, right of rectification* etc (see section 3 below) are restricted by the legal basis for processing, what reasons are there for considering the processing to be proportionate?

The rights of the data subjects are restricted in line with the processing requirements. This is proportionate as the processing is in pursuance of a public task/authority relating to law enforcement following any anti-social or criminal activities.

Signage advising of the use of CCTV will be placed on the ANGUSalive Countryside Rangers Base and public toilet extension at Forfar Loch Country Park.

What reasons are there for considering the processing is necessary to achieve the stated purpose and that there are no other reasonable ways to achieve that purpose?
The recorded images will be used for crime prevention /detection, identifying antisocial behaviour and public safety. The use of CCTV is the minimum required for gathering images in a reasonable and proportionate operation. This removes the need for corroboration, removes ambiguity and provides quality, accurate evidence.
What measures have been taken to ensure the personal information collected is both adequate to achieve the purpose of the processing and limited to on that information which is necessary to achieve the purpose?
Camera positions are set to capture appropriate images of incidents occurring around the toilet extension at ANGUSalive Countryside Rangers Base at Forfar Loch Country Park. The images will be date stamped and timed and a suitable maintenance regime will be in place. All images are subject to restrictions on the period of time they can be retained. Temporary portable toilet units have previously been provided in near proximity to the ANGUSalive Countryside Rangers Base at Forfar Loch Country Park. The units attracted significant levels of vandalism and antisocial behaviour which led to them being removed prematurely. It is considered prudent to ensure some form of surveillance is provided to target this type of behaviour and reduce it.

What measures have been taken to ensure the information is accurate and is kept up to date?
This is not relevant to recorded CCTV data as the images have no requirement to be updated.

Section 3 – Protecting Data Subject Rights

How will the right of the subject to be informed be met?
Signage at the CCTV camera site and statement of intent to record.
If data subjects retain a right of **access** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Rights to access the data will be in accordance with the right to a Subject Access Request under the General Data Protection Regulation. This Subject Access request can be made through ACCESSLine or online through the Council's website.
If data subjects retain a right to **rectification** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable

If data subjects retain a right to **erasure** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Rights to erase the data will be in line with Angus Council's privacy statement available on the Council website. This can be accessed on the following link: Angus Council Full Privacy Statement and contact details to allow this right to be exercised are available at the following link: Angus Council Privacy Statement - Contact Details
If data subjects retain a right to **data portability** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If data subjects retain a right to **restrict processing** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?
Not applicable.
If data subjects retain a right to **object** under the legal basis on which their data is processed, what arrangements are in place to enable data subjects to exercise that right?

Not applicable.
If some of the processing will be carried out by third party data processors, are there adequate contracts or service level agreements in place specifying the requirements for the processes undertaken, data sharing limitations, security requirements, and duties in relation to data subjects' rights? What arrangements are in place for monitoring compliance and reporting breaches?
Any data required by Police Scotland will be passed over, [redacted] All compliance requirements for handling data once passed over to Police Scotland are in line with their policies and procedures.
Is the personal data held and processed only within the UK or the European Economic Area? If not, what safeguards are in place to ensure the security, integrity and confidentiality of the data?
The data is held and processed within the UK.
If the processing covered by this DPIA is considered to pose a high risk in the absence of mitigation, has there been prior consultation with the Information Commissioner? What was the outcome of that consultation?
The information referred to in this DPIA is not deemed high risk.

Section 4 – Data Protection Risk Assessment

Use this section to identify the risks to the rights and freedoms of data subjects posed by the processing covered in this DPIA.

There are four main sources of risk which need to be considered:

- Illegitimate access to data
- Undesired modification of data
- Disappearance or destruction of data
- Inappropriate or uncontrolled sharing of data

For each of these categories, identify where in the processing the risk of a breach might arise and how it might arise. For each risk you need to quantify the:

- Likelihood of a breach occurring
  (1=negligible, 2=low, 3=moderate, 4=high, 5=extremely likely)
- The severity of the impact of a breach on the data subjects rights and freedoms
  (1=negligible, 2=minor, 3=moderate, 4=major, 5=catastrophic)
- The overall risk score (likelihood multiplied by severity)

You should then list the actions you will take to mitigate or eliminate each risk. The aim is to demonstrate that you have designed the process in such a way as to prevent or minimise the risk of a breach occurring.

If the overall score for any risk is 15 or more then you must seek prior consultation with the Data Protection Officer before implementing the processing covered by this DPIA.

Add rows to the tables as necessary.

1.1 Illegitimate Access

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Recording footage accessed by unauthorised staff.	2	2	4	Staff training on ensuring data is kept secured. Recording and reviewing equipment kept in a secure area.
Footage [redacted] for transfer to third party.	1	2	2	[redacted]

1.2 Undesired Modification

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Not applicable.				

1.3 Disappearance or Destruction

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Footage is deleted in error.	2	1	2	As data would subsequently be automatically deleted there are on further mitigation required.
Footage is deleted intentionally.	1	1	1	Where it is found that data had been deliberately deleted disciplinary action would be taken.

1.4 Inappropriate or uncontrolled sharing

Risk Description	Likelihood	Severity	Score	Mitigation Actions
Recorded footage is distributed to a wider audience.	1	2	2	Only authorised officers (as detailed in the DPIA) to view footage. Any inappropriate sharing would result in disciplinary action

Section 5 – IT advice

If the DPIA relates to a new system or app, IT advice is required to be noted here:

Section 6 – Data Protection Officer's Advice

I note the CCTV has been erected to reduce crime and associated fear of crime. It will also assist in provision of evidence, protection of property, assistance in civil claims, assistance in public health and safety. The data doesn't include personal data concerning any other individuals and will only record images of the subject.

The recording will only be accessed by Property Assets Maintenance Team, Clerk of Works or by ANGUSalive Countryside Rangers staff and their line management [redacted]

The information will only be shared with Police Scotland in the event of a request regarding a particular crime.

Police Scotland will still require to use the Data Protection Crime Investigation form to access any recording.

[redacted]

Notices will be visible to members of the public that CCTV is in operation and statement of intent to record.

Final decision if Data Controller's advice is contrary to the proposed processing

Section 7 – Outcome of Consultation with Data Subjects (if applicable)