Please contact the appropriate information asset owner/assistant as detailed in the information asset register if you require any support in completing this template and to sign off solutions to privacy risks.

Privacy Impact Assessment (PIA)
The SGC 'Privacy Impact Assessment Policy and Procedure' requires officers responsible for

Initiative name	**South Gloucestershire Community Safety Cameras - Downend**		
Responsible Officer	**Paul Worsley**	**Information Asset Owner**	**Robert Walsh**
Version and date	**1ST Version 04.02.20**		

The following screening questions will identify if a privacy impact assessment (PIA) is required. Answering 'yes' to any question will require a PIA to be completed. You may expand on the answers as work progresses.

No	Question	No	Yes	Comments
1	Will the initiative involve the collection of new information about individuals?		*	The Community Safety Cameras will be used for the gathering of live CCTV footage within Downend High St.
2	Will the initiative compel individuals to provide information about themselves?		*	The Community Safety Cameras will collect information about persons as and when they are being recorded. It is not a requirement of recorded individuals to provide additional information about themselves.
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? NB. This includes individuals who have previously accessed information but now work for a different organisation.		*	Information sharing agreements such as the SLA and Tier 2 agreement are currently in place to define parameters under which information can be shared.
4	Will you be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		*	The Community Safety Cameras will be used to record the behaviour of individuals who are either committing offences and/or behaving in a manner which may be deemed as threatening to the general public.
5	Does the initiative involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		*	The cameras will be high definition IP cameras offering enhanced night vision capabilities and increased resolution. The cameras will be used to record the behaviour of individuals who are either committing offences and/or behaving in a manner which may be deemed as threatening to the general public.
6	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		*	The initiative may result in information being passed to the Police and investigations being made against them in line with the council policies.

7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.		*	Community Safety Cameras may record criminal behaviour and include collateral intrusion from members of the public.
8	Will the initiative require you to contact individuals in ways which they may find intrusive i.e. invasive, indiscreet, interfering or upsetting?		*	We may use the information to pass to the Police in line with the council's information sharing agreements.

If all questions have been answered 'no' a copy of this document should be retained in accordance with our records retention policies and as the initiative develops reference made to the screening questions in case any answers change to 'yes'. If any question has been answered 'yes' please continue to complete the rest of this template.

Step one – Identify the need for a PIA

Initiative outline *Note – explain what the initiative aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find this information in management reports, committee papers, a project mandate, brief or PiD.*	South Gloucestershire Council will use the Community Safety Cameras to record the behaviour of individuals who are either committing offences and/or behaving in a manner which may be deemed threatening to the general public and/or operatives. South Gloucestershire Council have recently completed the process of upgrading their existing Community Safety Cameras from analogue to IP. This upgrade involved the implementation of high definition cameras offering an increased image resolution and advanced lighting features. The upgrade was necessary as IP network systems can be expanded more easily than analogue systems thus allowing scalability to meet the growing need. In addition, the cost of IP hardware has considerably decreased over the years whilst the development in analogue technology is slowly coming to an end.
Why is a PIA required? *Note – this can draw on your answers to the screening questions.*	A Privacy Impact Assessment (PIA) is required to help identify, minimise and address the privacy risks associated with the implementation of Community Safety Cameras.

Step two – Describe the information flows

Information flows *Note – describe how personal information is collected, stored, used and deleted explaining what information is used and what is it used for and who has access to it. It may also be useful to refer to process diagrams or another way of explaining data flows. To obtain a full understanding of information flows it is important that you consider <u>all</u> of the following information:* • *How many individuals will be affected?* • *How information is collected?* • *Why is information collected?* • *How will the information be stored?* • *For how long will the information be stored?* • *Where has information come from?* • *Who will have access to the information?*	South Gloucestershire Council currently have operational procedure documents and service level agreements in place with its external provider of CCTV Monitoring, Bristol City Council. **How many individuals will be affected?** Individuals affected by this initiative will be all pedestrians and vehicles who enter the areas covered by the CCTV system. **How is the information collected?** Information collected consists of visual recording of images captured by closed circuit television cameras. CCTV footage is recorded in 1080p HD resolution at 25/30fps or less to Network Video Recorders or Digital Video Recorders. **Why is the information collected?** The information is collected for the purpose of the prevention and detection of crime and disorder and general public safety. This forms part of the authorities aim to use community safety cameras to help prevent and reduce crime and disorder in the South Gloucestershire area making it a safe environment to live, work and visit.

• *How will information be deleted?*
• *Can analysis or reporting of anonymised data sets identify an individual?*
• *Can combining various sets of data result in the identification of an individual?*
• *Potential risks with the information flow?*
• *For use of existing data does the consent form/s used to collect the original data, and the associated privacy notices, cover the use of the data being considered by the initiative.*
	• To reduce the fear of crime and provide reassurances to the general public
	• To detect, deter and prevent crime by :
	  ○ assisting in the prevention of crime
	  ○ helping to identify, apprehend and prosecute offenders
	  ○ providing evidence to take criminal and civil action in the courts
	  ○ maintenance of public order
	  ○ reduce vandalism, graffiti, criminal damage and other nuisances
	  ○ reduce vehicle crime in the South Gloucestershire area and the public car parks
	  ○ to enable the Police to provide a more effective response
	
	How will the information be stored and for how long? The information will be securely stored by Bristol City Council as part of the contracted service provided by them, i.e. in such a way to provide continuity of evidence in accordance with their Codes of Practice. CCTV footage will be recorded directly to Network Video Recorders and securely stored for a maximum of 30 days. This 30 day retention period is proportionate to the nature of the data being captured. Remote access to the hard drive can also be gained via client software IVMS 4200 and Smart PSS from the council offices using a secure login
	
	Where does the information come from? The information will come from the recorded images captured by the 3 Community Safety Cameras situated within Downed High St. An assessment of the cameras location and view is conducted by the CCTV Officer at each new deployment. Any collateral intrusion is assessed and where necessary privacy masking is added to the cameras view.
	
	Who will have access to the information? Bristol City Councils emergency control rooms operators, South Gloucestershire Councils CCTV Officer and/or associated staff undertaking or supporting this officers duties. Police will also be able to gain access where requests are made and for the purpose of the Regulation of Investigatory Powers Act 2000 authorisation as per the policy “Bristol City Council / Avon and Somerset Police CCTV Protocols”.
	
	As SGC’s SLA with Bristol City Council states, will disclose recording to others as required by law but not otherwise (except that Bristol City Council when complying with Subject Access Requests will exercise discretion concerning the privacy masking of images relating to others and it may disclose these images

	where it considers it reasonable to do so). Bristol City Council may also make voluntary disclosure to others in certain circumstances such as insurance companies or a solicitor acting on behalf of someone who has been charged with a criminal offence for disclosure of material which may be admissible in the proceedings relating to that offence. Access to the BCC's Emergency Control Centre is restricted as per the details provided in the SLA. **How will information be deleted?** CCTV footage will be recorded directly to the Network Video Recorders and securely stored for a maximum of 30 days before being automatically deleted, unless information is requested, retrieved and copied by the Police as evidence relating to investigations. The 30 day retention period is proportionate to the nature of the data being captured. **Can analysis or reporting of anonymised data sets identify an individual? Can combining various sets of data result in the identification of an individual?** Analysis of anonymised datasets would be unable to identify any individuals. It is not thought likely that any combining of various sets of data would result in the identification of an individual. **Potential risks with the information flow?** Inappropriate access and/or disclosure of captured images, and data being held about individuals longer than necessary. However, these risks are mitigated against in the existing SLA between SGC and BCC which details the process and procedures. **For use of existing data does the consent form/s used to collect the original data, and the associated privacy notices, cover the use of the data being considered by the initiative?** Not applicable to this initiative. However, clear compliant signage within the High St will reflect that CCTV data is recorded for the prevention and detection of crime and the general wellbeing of users to the area.
Advice sought and consultation *Note – explain what practical steps you will take to ensure that you identify and address privacy risks. Who needs to provide advice? Who should be consulted, internally and externally? How will you obtain advice and carry out consultation?*	Continued legal advice is undertaken with regard to the use of the Community Safety Cameras within South Gloucestershire. The Community Safety Cameras and compliance with the Data Protection laws are reviewed annually and the appropriate advice is sought to mitigate any risks that may arise. Quarterly review meetings are also in place with external providers to ensure contractual agreements are continued to be met.

Step three – identify the privacy related risks

Note – identify the key privacy risks and the associated legislative compliance and corporate risks. Corporate and compliance risks identified should be referred to the Information Asset Owner.

Annex 1 provides an extract from the ICO's code of practice to help you identify where there is a risk that the initiative will fail to comply with the Data Protection Act or other relevant legislation, for example the Human Rights Act.

	Consequence		
Privacy risk/ issue	**Identify risks to individuals**	**Identify legislative compliance risks**	**Identify associated organisation/ corporate risk**
The initiative will involve the collection of new information about individuals	Information that is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.	Non-compliance with the DPA resulting in enforcement action	Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business
The initiative will compel individuals to provide information about themselves	Inadequate disclosure controls increase the likelihood of information being shared inappropriately.	Non-compliance with the DPA resulting in enforcement action Human Rights Act (Section 8)	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage
Information about individuals will be disclosed to organisations or people who have not previously had routine access to the information	There may be concern that other organisations may not have the same level of security as SGC.	Non-compliance with the DPA resulting in enforcement action Non-compliance with the PECR	Data losses which damage individuals could lead to claims for compensation
The information about individuals will be used for a purpose it is not currently used for, or in a way it is not currently used	The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.	Non-compliance with the DPA resulting in enforcement action Non-compliance with the PECR	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. This can also cause damage and distress to data subjects.
The initiative involves using new technology which might be perceived as being privacy intrusive	New surveillance methods may be considered an unjustified intrusion on their privacy if not necessary and proportionate.	Non-compliance with human rights legislation	The use of new technology may cause increased concern causing people to avoid engaging with the organisation

The initiative will be used in making decisions or taking action against individuals in ways that can have a significant impact on them	Measures taken against individuals as a result of collecting information about them might be seen as intrusive.	Non-compliance with human rights legislation	Public distrust about how information is used can damage an organisation's reputation and lead to loss of business
The initiative will require individuals being contacted in ways that they may find intrusive i.e. invasive, indiscreet, interfering or upsetting	Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information	Non-compliance with human rights legislation	Could result in mistrust and a lack of confidence in the council by the customer
Increased camera resolution resulting in higher risk of Collateral intrusion	Accidental capture and release of personal data – possibly causing damage and or distress to the individual	Illegal disclosure of personal data, i.e. non-compliance with the DPA and Article 8 of Human rights act.	ICO Enforcement action, including monetary penalty of up to the sterling equivalent of €20,000,000.
Lack of clear Signage to clearly indicate overt surveillance may be taking place	Completely unaware of the images being captured.	Unwarranted intrusion and infringement of data subjects human rights. Also non-compliance with RIPA.	ICO Enforcement action, including monetary penalty of up to €20,000,000.

Step four – identify privacy solutions

Note – describe the action you could take to reduce risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).
You will need to score the privacy risk by multiplying the impact of the risk happening (1-3) by the likelihood of the risk happening (1-3) using the key shown in the table below. Once you have identified the solutions (mitigating actions/ opportunities) to manage or mitigate the privacy risk you need to calculate the residual score. Any privacy risk with a residual score of 6 or more should be considered high risk by the Information Asset Owner.

	Impact (I)	***Likelihood (L)***	***Score (S)***
1	*No or slight impact*	*Unlikely to happen*	*I x L*
2	*Significant impact*	*Possible to happen*	
3	*Major impact*	*Highly likely to happen*	

Further guidance is available on the insurance, risk and opportunity management intranet site

Ref	***The Risk*** ***What can happen and how it can happen***	***Consequence / benefit of event happening***	***Inherent Risk***			***Mitigating Actions / Opportunities***	***Residual Score***			***Further Action Required***	***Risk Owner***	***Open/ closed***
			I	***L***	***S***		***I***	***L***	***S***			
1	Damage (intentional/accidental) to community safety cameras in situ	Financial loss of camera to local authority.	2	2	4	Cameras are installed approximately 6 metres above the ground on dedicated posts or alternatively attached to buildings to deter vandalism. It is anticipated that any (accidental/intentional) damage caused to the cameras would be covered by the council's corporate insurance arrangements.	2	1	2	None	CCTV Officer	Closed

Ref	*The Risk* *What can happen and how it can happen*	*Consequence / benefit of event happening*	*Inherent Risk*			*Mitigating Actions / Opportunities*	*Residual Score*			*Further Action Required*	*Risk Owner*	*Open/ closed*
			I	*L*	*S*		*I*	*L*	*S*			
2	The initiative will involve the collection of new information about individuals	Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business	1	2	2	The current contractual arrangements and processes covering the Community Safety Cameras reflects robust data collection, storage and disposal processes.	1	1	1	Ensure that current contracts/processes that are extended have equally robust arrangements with any new suppliers and are regularly reviewed.	CCTV Officer	Open
3	The initiative will compel individuals to provide information about themselves	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage	2	1	2	Ensure that process is implemented and monitored as outlined above	1	1	1	Clear signage – Ongoing checks for consistency	CCTV Officer	Open

Ref	The Risk What can happen and how it can happen	Consequence / benefit of event happening	Inherent Risk			Mitigating Actions / Opportunities	Residual Score			Further Action Required	Risk Owner	Open/ closed
			I	L	S		I	L	S			
4	Information about individuals will be disclosed to organisations or people who have not previously had routine access to the information	Data losses and/or breaches such as ID theft, victimisation, targeting etc impacting on the safeguarding of residents personal data. The damage to individuals could lead to claims for compensation and enforcement action taken by the ICO	2	1	2	Police routinely have access to the information captured by the Community Safety Cameras as part of the access arrangements currently in place for the prevention, detection and investigation of crime and disorder. The current process complies with the DPA. All covert surveillance and monitoring complies with RIPA and human rights legislation. Up to date policies and procedures are in place to ensure the necessary RIPA applications are completed correctly and within the guidance of the law. BCC operators would have access to the information as part of the contractual arrangements to live proactive monitoring of the cameras. No other persons or organisation will have access to the information.	1	1	1	None	CCTV Officer	Closed

Ref	*The Risk* *What can happen and how it can happen*	*Consequence / benefit of event happening*	*Inherent Risk*			*Mitigating Actions / Opportunities*	*Residual Score*			*Further Action Required*	*Risk Owner*	*Open/ closed*
			I	*L*	*S*		*I*	*L*	*S*			
5	The information about individuals will be used for a purpose it is not currently used for, or in a way it is not currently used	Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage	2	1	2	The information captured about individuals will be used for the purpose of preventing and detecting crime and disorder and protecting the general public.	1	1	1		CCTV Officer	Closed

Ref	The Risk What can happen and how it can happen	Consequence / benefit of event happening	Inherent Risk			Mitigating Actions / Opportunities	Residual Score			Further Action Required	Risk Owner	Open/ closed
			I	L	S		I	L	S			
6	The initiative involves using new technology which might be perceived as being privacy intrusive	The use of new technology and collateral intrusion on innocent bystanders may cause concern.	1	2	2	The capabilities of the IP cameras implemented increase the risk of collateral intrusion from innocent bystanders. The Home Office Surveillance CCTV Code of Practice 2013 makes it clear that 'an individual can expect to be the subject of surveillance in a public place, as CCTV, for example is a familiar feature in places that the public frequent'. An individual can, however, rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place. Clear signage is in place advising individuals that they are entering an area which is covered by CCTV for the purpose of public safety. Legal advice has been sought and agreed relating to the wording of these signs.	1	1	1	Ensure mitigating measures such as privacy masking is used and affected individuals are notified prior to new installations. Ensure suitable signage is in place to advise the general public of the CCTV in operation.	CCTV Officer	Open

Ref	*The Risk* *What can happen and how it can happen*	*Consequence / benefit of event happening*	*Inherent Risk*			*Mitigating Actions / Opportunities*	*Residual Score*			*Further Action Required*	*Risk Owner*	*Open/ closed*
			I	*L*	*S*		*I*	*L*	*S*			
7	The initiative will be used in making decisions or taking action against individuals in ways that can have a significant impact on them	Public distrust about how information is used can damage an organisation's reputation and lead to loss of business	2	1	2	Decisions will be made and action will be taken in ways that can have a significant impact on an individual where the behaviour of that individual presents a risk to public safety or constitutes a criminal offence. The use of the cameras to prevent and detect crime and disorder will be made clear using signs throughout the covered area. The use of CCTV footage as evidence to tackle community safety issues demonstrates a commitment to the safety and wellbeing of the general public in line with our statutory duties. Robust processes and procedures are in place to ensure public trust in the operation of the cameras is compliant with the data protection legislation.	1	1	1	Ensure future arrangements /contracts with operator remain compliant with the DPA.	Paul Worsley	Open

Ref	*The Risk* *What can happen and how it can happen*	*Consequence / benefit of event happening*	*Inherent Risk*			*Mitigating Actions / Opportunities*	*Residual Score*			*Further Action Required*	*Risk Owner*	*Open/ closed*
			I	*L*	*S*		*I*	*L*	*S*			
8	The initiative will require individuals being contacted in ways that they may find intrusive i.e. invasive, indiscreet, interfering or upsetting	Public distrust about how information is used can damage an organisation's reputation and lead to loss of business	2	1	2	Individuals will only be contacted by partner agencies such as the Police where there are grounds in terms of an active investigation towards a perpetrator or a witness. Robust processes will be extended/put in place to ensure this only takes place in justifiable circumstances.	1	1	1	Ongoing checks	Paul Worsley	Open

Step five – sign off and record the PIA outcomes

Note – who has approved the privacy risks and solutions involved in this initiative? Who is responsible for implementing approved solutions?				
Risk	**Approved solution**	**Approved by whom and date**	**Who is responsible for implementing the solution?**	**Date implemented**
1 - 8	As outlined above	 5 Feb 2020	Paul Worsley	

Step six – Integrate the PIA outcomes back into the key documentation

Note – key documentation must be updated with PIA approved solutions.

Approved solution (mitigating actions/ opportunities)	PiD (yes/no - date)	Project plan (yes/no - date)	Risk/ issue log (yes/no - date)	Action/ decision log (yes/no- date)	Comms/ consultation plan (yes/no - date)	EQIA (yes/ no - date)	Consultation report (yes/no -date)	Committee/ decision report (yes/no - date)	Information Asset Register
	No	No	No	N/A	N/A	No	No	N/A	Yes

Annex 1

Principles of the Data Protection Act

This annex provides an extract from the Information Commissioner's Office 'Conducting Privacy Impact Assessments code of practice' to help you identify where there is a risk that the initiative will fail to comply with the Data Protection Act or other relevant legislation, for example the Human Rights Act. The principles listed are those set out in Schedule 1 of the Data Protection

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will individuals be told about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Is the information you are using of good enough quality for the purposes it is used for?
Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.
If you are procuring new software does it allow you to amend data when necessary?
How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.
What retention periods are suitable for the personal data you will be processing?
Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.
Will the systems you are putting in place allow you to respond to subject access requests more easily?
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Do any new systems provide protection against the security risks you have identified?
What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Will the project require you to transfer data outside of the EEA?
If you will be making transfers, how will you ensure that the data is adequately protected?