CARLISLE CITY COUNCIL

www.carlisle.gov.uk

Report to Executive

Agenda Item:

A.5

Meeting Date:	15 April 2019
Portfolio:	Finance, Governance and Resources
Key Decision:	Not Applicable:
Within Policy and Budget Framework	YES
Public / Private	Public

Title:	SURVEILLANCE CAMERA POLICY
Report of:	Corporate Director of Governance and Regulatory Services
Report Number:	GD.20/19

Purpose / Summary:

This Report presents the Council's proposed Surveillance Camera Policy. The Executive are asked to note advice from the Audit Committee and approve the said Policy.

Recommendations:

It is recommended that the Executive:

1 Take account of the Audit Committee's advice (Minute reference AUC.08/19) that the Policy include further information of the GDPR legislation on the right to erasure.

2 Review and approve the Surveillance Camera Policy.

Tracking

Audit Committee:	**18 March 2019**
Executive:	**15 April 2019**
Council:	**Not Applicable**

1. BACKGROUND

1.1 Through the delivery of its statutory and ethical duties, Carlisle City Council is committed to the health and well being of its staff, partners, contractors and members of the public. In undertaking those duties, the Council faces many risks to its staff, resources, and to its obligation to protect members of the public. To manage these risks, the Council considers the use of surveillance cameras as appropriate control measures, acknowledged as both deterrent and detection tools to potential incidents such as theft, damage or risk to safety.

1.2 To ensure the use of surveillance cameras is appropriate, including the collection, use, sharing, retaining and disclosing of captured images, the Council should have in place a Surveillance Camera Policy and associated procedural documentation.

1.3 This Policy is designed to set out the Council's commitment and approach to meeting the Home Office's Surveillance Camera Code of Practice, and the Information Commissioner's Office (ICO) Code of Practice for Surveillance Cameras and Personal Information.

1.4 Its implementation is also intended to ensure compliance with relevant legislative requirements such as the Human Rights Act 1998, the General Data Protection Regulation 2016/679 and the Data Protection Act 2018.

1.5 It details the Council's surveillance camera governance arrangements, processes and considerations which must be undertaken, prior to the procurement and deployment of any surveillance camera systems.

1.6 In addition to the Policy, a Surveillance Camera Operating Procedure Template has been prepared. This has been created based on the 12 Guiding Principles of the Surveillance Camera Code of Practice and requires Responsible Service Managers to operationally record their Principle compliant operating procedure.

1.7 This Policy sits within the Council's Information Governance Framework which sets out the Council's overarching approach to the governance of information it processes, and its commitment to embedding a Corporate culture of Information Governance. Review and compliance of the Surveillance Camera Policy will sit with the Council's Information Governance Manager and will be supported by Internal Audit.

1.8 The Policy applies to all surveillance camera activity undertaken by the Council and on its behalf. In addition, and in certain circumstances, it may also extend to third parties who are engaged to work with the Council, and those who request and receive surveillance camera footage for their own purposes.

1.9 Approval and implementation of this Policy, along with the completion of the Surveillance Camera Operating Procedures, will assist the Council in managing the risk of inappropriately deploying surveillance cameras or unlawfully processing the recorded images.

2. PROPOSALS

2.1 The Council is in the process of reviewing, revising and developing the Council's Information Governance Framework's associated policies; policies which relate to, have an impact on, or are designed to manage information. The Surveillance Camera Policy is the third policy to be developed and presented to Members for approval.

2.2 The operational use of surveillance camera systems will be consulted through Council subject matter experts, as per Section 6 of the Policy, to ensure timely and suitable input, compliance checks and sign-off.

2.3 The Audit Committee recommended (Minute reference AUC.08/19) that the Policy should include further information of the GDPR legislation on the right to erasure, owing to the potential privacy impacts due to surveillance camera recordings. This amendment has been made to Section 14 of the Surveillance Camera Policy for Member approval.

3. RISKS

3.1 Failure to embed an appropriate Surveillance Camera Policy risks the Council breaching Data Protection Legislation and surveillance camera industry guidance, which could result in damage to individuals and the Council. This could subsequently result in enforcement action against the Council, claims for compensation, reputational damage and a lost of trust of our customers and service users.

4. CONSULTATION

4.1 The Surveillance Camera Policy has been considered by the Governance Sub-Group, the Senior Management Team, the Portfolio Holder for Finance, Governance and Resources and the Audit Committee.

5. CONCLUSION AND REASONS FOR RECOMMENDATIONS

5.1 The existence and implementation of an approved Surveillance Camera Policy will serve as evidence to our customers, staff and regulators of the Council's commitment and approach to protecting them as well as its assets, whilst safeguarding privacy. Approval of this Policy and the appended Operating Procedure will ensure the Council manages the risks associated with the deployment of surveillance cameras, and the recording, processing and sharing of personal information for appropriate purposes which may arise.

6. CONTRIBUTION TO THE CARLISLE PLAN PRIORITIES

6.1 To support the Council in protecting its, staff, assets, and resources which underpin the delivery of the Council's corporate priorities and statutory services to its customers and service users.

Contact Officer:	**Aaron Linden**	**Ext:**	**7355**

Appendices attached to report: **Appendix 1 – Surveillance Camera Policy**

Note: in compliance with section 100d of the Local Government Act 1972 the report has been prepared in part from the following papers:

- **None**

CORPORATE IMPLICATIONS:

LEGAL – The Council is required to have a Surveillance Camera Policy in place to govern its use. This Policy has been drafted in order to meet the requirements of the relevant Codes of Practice.
FINANCE – There are no direct financial implications arising from this report.
EQUALITY – None
INFORMATION GOVERNANCE – Having a Surveillance Camera Policy in place which requires Responsible Service Managers to record their methods of compliance with the 12 Guiding Principles, is fundamental to ensuring the Council appropriately utilises surveillance cameras to protect its staff, assets and members of the public, whilst safeguarding privacy.

CARLISLE CITY COUNCIL

www.carlisle.gov.uk

Carlisle City Council

Surveillance Camera Policy

Original version number	0.1
Version number	0.1
Version issue date	XX/XX/XXXX
Supersedes	XXXX
Reviewed by	XXXX
Date reviewed	XXXX

Contents

1. Introduction

Carlisle City Council is committed to respecting individuals' right to privacy and supports their entitlement to go about their business. The Council must however balance this right of privacy against the requirement to protect members of the public, to prevent and detect crime and, to protect its assets such as staff, property, equipment and vehicles.

In meeting these requirements, the Council acknowledges the benefits of deploying surveillance cameras as deterrents, as well as a means of live monitoring and information gathering. Appropriate surveillance cameras can assist in successfully identifying an individual, whether they are a culprit, witness or victim, and footage can be used as proof of wrong doing, or proof of innocence.

This Policy is designed to support the Council through the surveillance camera assessment process, to decide when surveillance cameras should be deployed and, to ensure that the Council complies with the Home Office's Surveillance Camera Code of Practice (issued under the Protection of Freedoms Act 2012), and the Information Commissioner's Office (ICO) Code of Practice for Surveillance Cameras and Personal Information.

This Policy sits within the Council's Information Governance Framework which sets out the Council's overarching approach to the governance of its information and its commitment to embedding a Corporate culture of Information Governance.

2. Purpose

This Policy sets out the Council's approach to procuring, deploying and utilising surveillance cameras. It is designed to ensure that staff who are responsible for surveillance on behalf of the Council are fully aware of the legal requirements, appropriate purposes and considerations relating to surveillance cameras.

Each surveillance camera system will have its own purpose and specific objectives therefore, each must be assessed against this Policy by the Responsible Service Manager, to ensure it is compliant.

Appropriate use of surveillance cameras will include some of the following:

- Protecting Council officers and the public on Council property.
- Deterring and detecting crime and anti-social behaviour.
- Assisting in the identification of and apprehension of offenders.
- Deterring violent or aggressive behaviour towards Council officers.
- On-site traffic and car park management.
- Monitoring traffic movement.
- Identifying those who have contravened parking regulations.
- Assisting in traffic and planning regulation enforcement.
- Protecting council assets, property and surveying buildings for the purpose of maintenance and repair.
- Assisting in grievances, formal complaints and investigations.

3. Scope

This Policy and associated procedures apply to all camera surveillance carried out by the Council, whether it relates to staff, contractors or members of the public, including:

- Surveillance Cameras
- Body Worn Video (BWV)
- Automatic Number Plate Recognition (ANPR)
- Unmanned Aerial Systems (UAS) (Drones)
- Any other surveillance systems that capture footage or images of individuals

All staff and third parties who are engaged to work with the Council involving the use of surveillance must adhere to this Policy. It will also apply to third parties whom the Council shares surveillance footage with, whether through normal working arrangements or through specific requests.

This Policy is limited to the governance arrangements for surveillance cameras systems only. It is not designed to cover other forms or surveillance such as GPS trackers within vehicles and ICT equipment, recordings made by the Council's ICT system such as emails and internet usage, noise recording or social media information gathering.

Whilst it will be relevant when overt surveillance cameras are used, this Policy is also not designed to cover authorisations in relation to directed covert surveillance in accordance with The Regulation of Investigatory Powers Act (RIPA) 2000 or the Investigatory Powers Act 2016. Any use of overt surveillance cameras for pre-planned directed covert surveillance must comply with this Policy, the codes of practices referenced at Section 1, and the Home Office's Covert Surveillance and Property Interference Code of Practice 2018.

4. Objectives

The objectives of this Policy are to:

- Create and maintain an awareness of the Right to Privacy (Article 8, Human Rights Act 1998) as an integral part of the day to day business.
- Ensure that employees are aware of and fully comply with the relevant legislation and understand their own responsibilities when undertaking surveillance camera activities.
- Ensure that all employees acquire appropriate authorisations when undertaking surveillance camera activities.
- Store, archive and dispose of sensitive and confidential surveillance camera information in an appropriate manner.

The Council will achieve this by ensuring that:

- Regulatory and legislative requirements are met.
- Awareness raising activities are undertaken in relation to camera surveillance.
- All breaches of privacy, actual or suspected, are reported and investigated.
- Processes and practices are regularly reviewed.

- In relation to surveillance of staff, the Information Commissioner's Office Employment Practices Code of Practice is adhered to.
- A list of surveillance camera activity undertaken by Responsible Service Managers is managed and kept up to date (Appendix 1).

5. Data Protection Impact Assessment

Prior to the procurement of any surveillance camera systems, a needs assessment must be undertaken to consider the following:

- assessment of need
- purpose and objectives of the surveillance
- less intrusive alternative options that may achieve the same objectives
- locations of cameras
- impact to privacy
- cost

Carlisle City Council's Data Protection Impact Assessment (DPIA) covers these points therefore, is considered suitable as an operational assessment and a DPIA. As stated in the Council's Data Protection Policy, A Data Protection Impact Assessment (DPIA) is a process designed to help identify and minimise the data protection related risks of a project to individuals. For the guidance, including the DPIA Template, please refer to the Council's Data Protection Impact Assessment Guide.

6. Procurement of Surveillance Camera Equipment

Carlisle City Council will not procure surveillance cameras if there are cheaper, less intrusive and more effective methods of meeting the determined objectives.

Alternative ways of meeting the determined objectives will be considered as part of the Data Protection Impact Assessment with any reasons for them not being suitable, recorded. On the basis that surveillance cameras are considered the only suitable solution, consultation on the DPIA must be undertaken with the following subject matter experts for compliance checks and additional input or advice before any procurement process and subsequent installation:

- Property Services
- Information Governance Manager
- ICT Services
- Human Resources (when the camera surveillance relates to staff)
- Legal Services
- Policy and Communications (for equality considerations)

Furthermore, any purchase of surveillance camera equipment must be completed with regard to the Procurement Policy and with reference to the Council's Procurement Team as appropriate to ensure cost efficiency, an appropriate tender process and compliance with Council procedure.

Officers must ensure any equipment purchased is fit for purpose to meet the objectives it was purchased for to ensure the surveillance can be considered necessary.

7. Deployment of Surveillance Cameras

It is vital that as part of the Data Protection Impact Assessment, appropriate consideration is given to the necessity for surveillance cameras, and to assess any impact of them on the privacy of individuals using the areas where cameras are to be deployed. Cameras are not to be installed in such a way that they can investigate private space such as inside private dwellings.

Covert cameras are also not normally to be deployed into areas highly used by staff or the public (and will in all cases be deployed following a RIPA authorisation).

Surveillance cameras will not be operated in toilets, private offices or changing rooms, unless this is necessary for the investigation of a serious crime or there are circumstances in which there is a serious risk to health and safety or to the operation of the Council's business. CCTV will be used in this way only where it is a proportionate means of achieving the aim in the circumstances.

Some Council laptops with built in webcams can enabled to allow the Council to view staff whilst they are, for example, working from home. This facility is not enabled and will not be, ensuring no risk of invasion of privacy.

Concealed and unsigned cameras within property may on rare occasions be deployed in areas of high security where there is no legitimate public access and where staff access is controlled and restricted (for example, an IT server room or secure plant room). Staff who normally work in these areas should, where appropriate, be informed of the location of these cameras, their purpose and where the monitor to view the images is kept.

There is also a clear requirement for all surveillance camera schemes to have an effective maintenance schedule and to be operated in accordance with relevant guidance. Property Services alongside Council officers procuring and deploying surveillance camera equipment need to ensure these requirements are fully met.

Carlisle City Council does not deploy 'dummy' cameras as they give a false sense of security to the public who may otherwise have avoided an area not under "real" monitoring.

Council officers are not to purchase cameras that can be used for monitoring audio conversations or be used to talk to individuals without sign-off by a member of the Senior Management Team, as this is normally considered an unnecessary invasion of privacy. When such surveillance camera systems are capable of audio recording, this facility must be de-activated.

Once any new cameras have been installed, a copy of a map or building plan showing the location of the surveillance cameras should be sent to Property Services as part of the maintenance and repair register.

8. Council Operated Surveillance Cameras

Staff operating Council surveillance cameras systems are responsible for operating the equipment in accordance with all requirements set out in current legislation, this policy document, relevant guidelines, codes of practice and operating procedures. Council officers operating surveillance camera systems must be familiar with the requirements of information governance and must complete the council's relevant information governance eLearning courses.

Council officers involved in the use of surveillance camera systems shall report any misuse to the Responsible Service Manager and shall cooperate with any investigation by them. The Responsible Service Manager shall investigate any reported misuse of a surveillance camera system and report it immediately to the Senior Management Team and, if personal data has been compromised, the Information Governance Manager

Staff operating surveillance camera systems shall be responsible for bringing any equipment faults to the Responsible Service Manager's attention immediately.

9. Joint/ Third Party/ Independently Operated Surveillance Cameras

For surveillance camera systems procured by Carlisle City Council that are located in Operational Property other than those occupied solely by the Council (community centres, libraries, outsourced service providers, partner agencies etc). It is important that there is a clear understanding between the Council and the occupiers of the properties concerned as to associated roles and responsibilities assigned to each organisation – if any is shared – and what the surveillance camera systems may be used for.

Responsible Service Managers with the support of Legal Services in drafting the agreement need to ensure that any tenancy agreements or contracts include relevant clauses which clearly state the position with regards to operation of the surveillance camera system, for example:

- Full access is granted and on listed terms
- Shared specified access is granted and on listed terms
- No access is granted
- Any request for footage will be considered under Section 11 of this Policy

In circumstances where some form of access is granted, the contract clauses must cover the acceptable usage of the system and where the responsibility of each organisation lies in each case. A copy of this agreement must be appropriately stored and be accessible. The clauses must include the following:

- Decision to allow access, enable data sharing or to refuse
- Appropriate purposes of use
- Details of use/ access i.e. to view, download and/ or share footage
- The legislation, policies and guidance which need to be adhered to
- Restrictions on use
- Consequences of failure to appropriately use the system/ footage in accordance with this Policy and supporting documentation.

In addition, where some form of access is granted, the Council's Operating Procedure (Appendix 3) must be completed by both the Council and the third party, to refer to their respective individual usage.

In circumstances where the third party is a data processor under the General Data Protection Regulation as opposed to a joint data controller, a data processing agreement will be required in addition to the surveillance camera agreement.

10. Viewing, Access and Use of Footage and Images

The casual viewing or trawling of footage or images captured by a surveillance camera system is strictly forbidden. Viewings must only be carried out for a specific, legitimate purpose. It is however accepted that through viewing footage for legitimate purpose, other concerns, not directly related to the intended purpose of the viewing, may be identified. This Policy does not prevent these concerns from being acted upon, provided it is appropriate to do so, suitable assessment and investigation is undertaken and, relevant legislation is complied with.

On occasion Council services may wish to access images and recordings captured on surveillance camera systems as part of a legitimate investigation into criminal activities, civil claims, potential disciplinary matters, complaints, grievances or health and safety issues. Viewings and images will only be allowed/ released to a properly authorised investigating Council officer upon the submission of a formal request to the relevant Responsible Service Manager. The viewing request should include:

- The name of the authorising officer (i.e. Service Manager)
- The name and contact details of the person viewing images
- The reason for viewing the images

Viewing Requests should be made in a timely manner as the retention period for most surveillance camera systems in operation in the council is 28 days, unless there are exceptional reasons to hold the data for longer which are documented as part of the operating procedure.

A Responsible Service Manager may also instigate and authorise viewings and the use of footage they are responsible for without a request, if they believe an investigation is required in relation to an appropriate purpose.

11. Third Party Access Requests

Under Data Protection Legislation, data subjects, including staff, are entitled to know what personal information the Council holds about them, and they are entitled to receive a copy of their personal data. All such requests, known as Subject Access Requests (SARs), should be made through the Council's Information Governance Team at dataprotection@carlisle.gov.uk using the Council's SAR form, which can be found at Appendix 5 of the Employees Privacy Notice on the intranet or via your line manager.

Under the Freedom of Information Act 2000, people can request access to any recorded information (with certain exemptions) that the Council holds. However, if individuals are capable of being identified from the surveillance system footage then

it is personal information about the individual concerned and is unlikely to be disclosed in response to a freedom of information request, as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the Data Protection Legislation. All Freedom of Information requests relating to surveillance camera system images should be directed to the Council's Information Governance Team at information@carlisle.gov.uk.

On occasion, the police may request to view images taken from surveillance camera systems during the investigation of criminal activity. This is acceptable under the Data Protection Legislation. However, the police officer making the request must complete a Third-Party Request form (Appendix 2) available on the Council's website confirming that the information is needed for the detection or prevention of a specific crime. The form must be signed by a senior police officer and sent to the relevant Responsible Service Manager who will consider the request. Police officers are not permitted to trawl the Council's surveillance camera systems on the off chance of detecting a crime. Responsible Service Managers must use the CCTV Log Book and Incident Download Pack where it is deemed appropriate to provide footage in response to such a request.

In exceptional circumstances, for example, to support the investigation of serious crime where an urgent response is required by the Police, and where a senior police officer has not signed the viewing application form, the Responsible Service Manager has discretion to grant access to surveillance camera footage to a police officer on completion of the form.

Occasionally, insurance companies or solicitors will request footage, generally over disputes regarding damage to cars in car parks. As the footage may identify the individual drivers or vehicles involved it is classed as personal information. As stated above, copies of personal information can be requested by making a Subject Access Request under Data Protection Legislation. Ordinarily individuals are only entitled to information about themselves; however, in certain circumstances it is reasonable to include information about third parties, and this may be permitted by the Data Protection Legislation. Such circumstances may include where a third party has caused damage to you or your vehicle. All such requests must be made through the Council's Information Governance Team, who log all such requests and who may need to redact third party information. A record of all disclosures is kept in the Council's case management system.

As referred to at Section 9 of this Policy, in absence of appropriate tenancy agreements or contracts or, when no access has been granted to the third party, all requests for footage will be dealt with under this Section of the Policy, requiring the Third-Party Request form to be completed and sent to the relevant Responsible Service Manager who will consider the request.

12. Signage

All areas where surveillance cameras are in use should be clearly signed to comply with Data Protection Legislation. This is to advise people that they are about to enter an area monitored by surveillance cameras or to remind them that they are still in an area covered by surveillance cameras. The signs will also act as an additional deterrent. Surveillance camera signs should not be displayed in areas which do not

have surveillance cameras. Where ‘covert’ cameras have been authorised for deployment, signage will not normally be installed.

The surveillance camera signs should have a yellow background with all writing in clear black print and should carry the Council’s logo. The information on the sign should explain why the surveillance cameras are there, who operates them, a contact number to obtain information and, refer to the Council’s Surveillance Camera Privacy Notice. The signs, position and the message need to be adequate to enable people to easily read the information on them.

Members of staff should be made aware of surveillance cameras located in their work environment as part of their induction.

13. Disciplinary Offences and Security

Tampering with or misuse of cameras, monitoring or recording equipment, documents or recorded data by staff may be regarded as gross-misconduct and could lead to disciplinary action, which may result in dismissal or criminal prosecution.

Any breach of this policy document or relevant guidance will be regarded as a serious matter. Staff who are in breach of this instruction may be subject to action under the Carlisle City Council disciplinary procedures.

The responsibility for ensuing the security and proper use of the system will rest with the Responsible Service Manager of the system concerned. These officers will, in the first instance, investigate all breaches or allegations of breaches of security or misuse and will report their findings to the Senior Management Team.

The security of the surveillance camera equipment must be considered as part of the Data Protection Impact Assessment with consideration given to both technical and organisational measures. All surveillance camera devices must be encrypted, and footage must not be stored on mobile devices. The preferred location for footage and image files is the Council’s approved ICT locations.

14. Compliance with Data Protection

In almost all uses of surveillance cameras, personal data is either intended to be processed or, is indirectly processed through the pursuit of the systems objectives. All surveillance camera processing therefore needs to be done in accordance with Data Protection Legislation and the Council’s Data Protection Policy, with particular emphasis on adherence to the Data Protection Principles, rights of individuals and security.

To fulfil any of their rights, including the qualified right to have personal information recorded by surveillance camera systems erased, individuals should contact the Council’s Data Protection Officer at dataprotection@carlisle.gov.uk or call 01228 817200.

15. Roles and Responsibilities

Overarching roles and responsibilities in relation to Information Governance are contained within the Council's Information Governance Framework. In addition to those overarching roles, the Council also has the following roles and responsibilities, specifically in relation to surveillance cameras:

Responsible Service Manager

Each surveillance camera system must be managed by a Responsible Service Manager. In circumstances where a single system is used for different purposes, the default responsibility structure will consist of a corporate Responsible Service Manager who will still take the overall lead for the system. In addition, further Responsible Service Managers will be assigned to manage the secondary purposes for which the system is used for. The Responsible Service Manager role should be covered within job descriptions.

The role of the Responsible Service Manager is to:

- Ensure the use of the surveillance camera system is compliant with this Policy and that staff are aware of this Policy, its appendices and associated policies listed in Section 18 of this Policy.
- Complete and maintain the Surveillance Operating Procedure, ensuring staff are aware of it, adhere to its terms and receive appropriate training where necessary.
- Take operational responsibility for the surveillance camera system under their control and the appropriate recording, use and disclosure of footage and images.
- Contribute to the Council's maintenance and repair register – register of all surveillance cameras.
- Act as the service point of contact for all enquiries relevant to the surveillance camera systems they are responsible for, ensuring only authorised council officers can operate or view footage images.
- Deal with and respond to third party requests from the Police, releasing the information when appropriate and seeking advice and guidance as required.
- Investigate any reported misuse of a surveillance camera system and report it immediately to the Senior Management Team and the Information Governance Manager.
- Ensure any faults in the surveillance camera system equipment are reported and remedied at the earliest opportunity.
- Ensure when they leave their post their line manager is advised of the need to designate the role to another staff member.

Senior Responsible Officer

The role of the Senior Responsible Officer (SRO) is to deliver a corporate approach to the Council's responsibilities arising from the Protection of Freedoms Act 2012, ensuring due regard to the Home Office's Surveillance Camera Code of Practice. In addition, the SRO is required to support the Council in complying with the Information Commissioner's Office (ICO) Code of Practice for Surveillance Cameras and Personal Information.

The Council's Information Governance Manager (Data Protection Officer) has been designated as the Senior Responsible Officer, as per guidance from the Surveillance Camera Commissioner.

In accordance with Section 17 of this Policy, the Information Governance Manager will review the adequacy of this Policy and monitor compliance with it.

Information Support Officer

The role of the Information Support Officer is to:

- Centrally co-ordinate requests for access to surveillance camera footage and images, in conjunction with Council department contacts and ensure responses are processed appropriately and issued in a timely manner.

16. Training, Communication and Awareness

Relevant staff must receive training on the surveillance camera operating system to ensure it is used correctly and the risk of a data breach, including the availability of information, is managed.

The Council's mandatory Data Protection E-Learning training must be undertaken by Responsible Service Managers, system operators and staff who use information from the system prior to their involvement with the surveillance system.
Training relative to the surveillance camera operation must be undertaken on a refresher basis at appropriate intervals based on developments and associated risks.
Communication and awareness must be raised through normal working practices of the Council's policies and procedures in relation to surveillance cameras, any surveillance that will impact on staff and members of the public and, the Responsible Service Managers for each system.

17. Implementation and Compliance Monitoring

This Surveillance Camera Policy will be implemented and supported by the Senior Management Team, employees and non-employees representing the Council, and overseen and monitored by the Information Governance Manager.

New associated Procedures may be developed in collaboration with key subject matter experts, consulted through the Governance Sub-Group and the Senior Management Team and signed off by the Corporate Director of Governance and Regulatory Services. They will subsequently be considered as applicable under this Policy and circulated to relevant staff for awareness.

Implementation and adherence of this Policy will be monitored by the Information Governance Manager who will carry out two-yearly audits to ensure it is applied in practice.

18. Associated Procedures, Guidance and Documents

- Information Governance Framework
- Data Protection Policy
- Records Management Policy
- RIPA Policy
- Code of Conduct for Employees
- Code of Corporate Governance
- Social Media Policy
- Employee Privacy Notice
- Individual Privacy Notice (non-employees)

19. Further Information and Guidance

- Surveillance camera Code of Practice
- ICO SURVEILLANCE CAMERA Code of Practice
- ICO Data Protection Impact Assessment
- Regulation of Investigatory Powers Act Codes

20. Review

This Policy will be reviewed two-yearly following the implementation and adherence audits which will inform the review.

Appendix 1 - List of camera surveillance service and Responsible Service Managers

Surveillance Camera Locations	Service Manager
1. Fleet Vehicles 2. On Enforcement Officers 3. Mobile Units 4. Bousteads Grassing Depot 5. Supervisors' Office 6. Vehicle Workshops 7. Car parks and Recycling Sites	Neighbourhood Services Manager
1. Old Fire Station	Health and Wellbeing Manager
1. Crematorium 2. Richardson Street Cemetery 3. Hammonds Pond 4. Talkin Tarn 5. Bitts Parks Depots	Health and Wellbeing Manager
1. Customer Contact Centre	Customer Contact Manager
1. Computer rooms	ICT Services Manager
1. Business Interaction Centre, Paternoster Row	Regeneration Manager
1. Enterprise Centre	Building and Estates Manager
1. Accommodations	Homelessness Prevention and Accommodation Manager

Appendix 2 - Surveillance Camera Viewing/ Footage Request Form

CARLISLE CITY COUNCIL
www.carlisle.gov.uk

1 Applicant details

Name	
Position	
Organisation	
Address	
E-mail address	
Telephone number	

2 Footage required

System	
Date	
Time (Start and finish)	
Location	
Details of incident (if appropriate)	

3 Entitlement / purpose to view

Please confirm the purpose for making this request and detail the lawful / statutory basis for viewing the information	

Declaration

I understand that the surveillance camera footage is to be viewed in connection with the above incident only and that all information obtained is to be processed in line with the General Data Protection Regulation. Any future use of the surveillance camera footage/ evidence is to be used only for the purposes outlined above, unless you are lawfully able to use it for another purpose

Signed: Date:

4 Authorisation by Carlisle City Council Responsible Service Manager

Application	**Accepted / Refused** (please delete as appropriate)
Reason if refused	
Signed	
Name	
Date	

CARLISLE CITY COUNCIL

www.carlisle.gov.uk

Carlisle City Council

Surveillance Camera Operating Procedure

Original version number	0.1
Version number	0.1
Version issue date	XX/XX/XXXX
Supersedes	XXXX
Reviewed by	XXXX
Date reviewed	XXXX

Surveillance camera system	
Type of surveillance cameras	
Responsible Service	
Responsible Service Manager	
Primary operational objective	
Under Data Protection Legislation, what is the lawful basis for processing?	
Locations	1.
Number of cameras at each site	1.
Date of Installation	
Date of last review (purpose and equipment maintenance)	
Date of next review (purpose and equipment maintenance)	
Date of Data Protection Impact Assessment	

Signage 1. Location 2. Size 3. Clear/ easy to read 4. Operator stated? 5. Purpose stated? 6. Contact details? 7. Refers to surveillance camera privacy notice?	
Staff authorised to view surveillance footage?	
Staff authorised to sign-off use, downloads and disclosures of footage?	
What training and awareness have staff received?	
What are the retention periods for the footage?	
Staff authorised to delete images when retention period met?	
What security is applied to the system (organisational and technical)	
Are regular checks that the system is working scheduled and undertaken?	

EXCERPT FROM THE MINUTES OF THE AUDIT COMMITTEE HELD ON 18 MARCH 2019

AUC.08/19 SURVEILLANCE CAMERA POLICY

The Information Governance Manager reported (GD.17/19) that, through the delivery of its statutory and ethical duties, Carlisle City Council was committed to the health and wellbeing being of its staff, partners, contractors and members of the public. In managing the many risks faced in undertaking those duties, the Council considered the use of surveillance cameras to be appropriate control measures, acknowledged as both deterrent and detection tools to potential incidents such as theft, damage or risk to safety.

To ensure that the use of surveillance cameras was appropriate, including the collection, use, sharing, retaining and disclosing of captured images, the Council should have in place a Surveillance Camera Policy and associated procedural documentation.

The proposed Policy was designed to set out the Council's commitment and approach to meeting the Home Office's Surveillance Camera Code of Practice, and the Information Commissioner's Office (ICO) Code of Practice for Surveillance Cameras and Personal Information. Its implementation was also intended to ensure compliance with relevant legislative requirements such as the Human Rights Act 1998, the General Data Protection Regulation 2016/679 and the Data Protection Act 2018.

It detailed the Council's surveillance camera governance arrangements, processes and considerations which must be undertaken, prior to the procurement and deployment of any surveillance camera systems. In addition to the Policy, a Surveillance Camera Operating Procedure Template had been prepared, based on the 12 Guiding Principles of the Surveillance Camera Code of Practice, and which required Responsible Service Managers to operationally record their Principle compliant operating procedure.

This Policy sat within the Council's Information Governance Framework which set out the Council's overarching approach to the governance of information it processed, and its commitment to embedding a Corporate culture of Information Governance. Review and compliance of the Surveillance Camera Policy would sit with the Council's Information Governance Manager and be supported by Internal Audit.

The Policy applied to all surveillance camera activity undertaken by the Council and on its behalf. In addition, and in certain circumstances, it may also extend to third parties engaged to work with the Council, and those who requested and received surveillance camera footage for their own purposes.

The Information Governance Manager added that approval and implementation of the Policy, along with the completion of the Surveillance Camera Operating Procedures, would assist the Council in managing the risk of inappropriately deploying surveillance cameras or unlawfully processing the recorded images.

The Principal Auditor added that any area reviews would include the proposed Policy as part of the audit to ensure that each service area that used CCTV was compliant.

In response to questions the Information Governance Manager clarified that any signage requirements for surveillance cameras would be dealt with by the relevant service manager to comply with the Policy. With regard to GDPR requirements the Information Governance Manager explained that the Policy was in addition to the Council's Privacy Notice and a CCTV Privacy Notice.

The Committee felt that the GDPR requirements, particularly information on the right to erasure should be strengthened within the Policy

RESOLVED – That the Audit Committee had reviewed the Surveillance Camera Policy (GD.17/19) and recommend approval of the Policy to the Executive subject to the inclusion of further information of the GDPR legislation on the right to erasure.