CARLISLE CITY COUNCIL

www.carlisle.gov.uk

AGENDA

Executive

Monday, 15 April 2019 AT 16:00
In the Flensburg Room, Civic Centre, Carlisle, CA3 8QG

Apologies for Absence

To receive apologies for absence.

Declarations of Interest
Members are invited to declare any disclosable pecuniary interests, other registrable interests and any interests, relating to any item on the agenda at this stage.

Public and Press
To agree that the items of business within Part A of the agenda should be dealt with in public and that the items of business within Part B of the agenda should be dealt with in private.

PART A

To be considered when the Public and Press are present

A.1 NOTICE OF EXECUTIVE KEY DECISIONS **5 - 14**

(Non Key Decision)

The Notice of Executive Key Decisions, published on 15 March 2019, is submitted for information.

Key Decision (KD.07/19) - Sands Centre Redevelopment: The Deputy Chief Executive had been scheduled to submit a report on the Sands Centre Redevelopment to a special meeting of the Executive on 1 April 2019. The redevelopment of the Sands Centre is a large and multifaceted project. Whilst good progress has been made on developing the full capital and revenue implications of this project, governance advice strongly suggests that this is not an appropriate time to seek such a key decision from Executive (and consequently Council) on our future revenue and capital budgets. Following the City Council elections, a revised decision making timetable will be brought forward.

(Copy Notice herewith)

A.2 SCHEDULE OF DECISIONS TAKEN BY PORTFOLIO HOLDERS 15 - 16

(Non Key Decision)

A Schedule detailing a decision taken by the Leader under delegated powers is attached for information.

(Copy Schedule herewith)

Background Papers - as detailed within the Schedule

A.3 SCHEDULE OF DECISIONS TAKEN BY OFFICERS 17 - 20

(Non Key Decision)

A Schedule detailing decisions taken by Officers under delegated powers is attached for information.

(Copy Schedule herewith)

Background Papers - as detailed within the Schedule

A.4 JOINT MANAGEMENT TEAM **21 - 22**

(Non Key Decision)

The Minutes of the meeting of the Joint Management Team held on 11 March 2019 are submitted for information.

(Copy Minutes herewith)

A.5 SURVEILLANCE CAMERA POLICY **23 - 46**

(Non Key Decision)

The Corporate Director of Governance and Regulatory Services to submit a report presenting the Council's proposed Surveillance Camera Policy. The Audit Committee considered the matter on 18 March 2019.

(Copy Report GD.20/19 and Minute Excerpt herewith)

A.6 REGULATION OF INVESTIGATORY POWERS: UPDATE **47 - 102**

(Non Key Decision)

The Corporate Director of Governance and Regulatory Services to submit a report providing an update on the Council's use of the surveillance powers open to it under the Regulation of Investigatory Powers Act 2000 (RIPA). The Audit Committee considered the matter on 18 March 2019.

(Copy Report GD.19/19 and Minute Excerpt herewith)

Background Papers - The Home Office Guidance Documents referred to in the report are available on the relevant websites

PART B

To be considered when the Public and Press are excluded from the meeting

B.1 BIC PROJECT, PATERNOSTER ROW, CARLISLE

- Information relating to the financial or business affairs of any particular person (including the authority holding that information);

Members of the Executive

Councillor C W Glover (Leader)

Councillor Dr L Tickner (Deputy Leader, and Finance, Governance and Resources Portfolio Holder)
Councillor Ms A Quilter (Culture, Heritage and Leisure Portfolio Holder)

Councillor Miss L B Sherriff (Communities, Health and Wellbeing Portfolio Holder)

Councillor C J Southward (Environment and Transport Portfolio Holder)
Councillor A Glendinning (Economy, Enterprise and Housing Portfolio Holder)

Enquiries to:

Morag Durham - Tel: (01228) 817036 or
Morag.Durham@carlisle.gov.uk

Notes to Members:

Decisions made at this meeting, if not subject to call-in, will normally become live on 29 April 2019

CARLISLE CITY COUNCIL

www.carlisle.gov.uk

NOTICE

OF EXECUTIVE KEY DECISIONS

15 MARCH 2019

Notice of Key Decisions

This document provides information on the 'key decisions' to be taken by the Executive within the next 28 days. The Notice will be updated on a monthly basis and sets out:

Details of the key decisions which are to be taken;
Dates of the Executive meetings at which decisions will be taken;
Details of who will be consulted and dates for consultation;
Reports and background papers which will be considered during the decision making process;
Details of who to contact if further information is required
Details of where the document can be inspected
Details of items which the public may be excluded from the meeting under regulation 4(2) and the reason why
Details of documents relating to the decision which need not, because of regulation 20(3) be disclosed to the public and the reason why.

The dates on which each new Notice will be published are set below:

Publication Dates

30 April 2019	16 August 2019	17 December 2019
17 May 2019	13 September 2019	10 January 2020
21 June 2019	18 October 2019	7 February 2020
19 July 2019	15 November 2019	6 March 2020

Key decisions are taken by the City Council's Executive and these are usually open to the public. Agendas and reports and any other documents relevant to the decision which may be submitted can be viewed in the Customer Contact Centre at the Civic Centre, Carlisle or on the City Council's website (www.carlisle.gov.uk). Agendas and reports are published one week ahead of the meeting.

A Key Decision is an Executive decision which is likely –

(a) to result in the relevant local authority incurring expenditure which is, or the making of savings which are, significant* having regard to the local authority's budget for the service or function to which the decision relates;
(b) to be significant in terms of its effects on communities living or working in an area comprising two or more wards or electoral divisions in the area of the relevant local authority.

*significant expenditure or savings to the authority in excess of £70,000

The City Council's Executive Members are:

Councillor Glover –Leader
Councillor Dr Tickner – Finance, Governance and Resources Portfolio Holder
Councillor Ms Quilter – Culture, Heritage and Leisure Portfolio Holder
Councillor Miss Sherriff – Communities, Health and Wellbeing Portfolio Holder
Councillor Southward – Environment and Transport Portfolio Holder
Councillor Glendinning – Economy, Enterprise and Housing Portfolio Holder

Should you wish to make any representations in relation to the items being held in private or If you require further information regarding this notice please contact Democratic Services on 01228 817039 or committeeservices@carlisle.gov.uk.

Index of Active Key Decisions

		Date Decision to be considered:	Date Decision to be taken:
KD.05/19	2018/19 Provisional Outturn Reports		29 May 2019
KD.07/19	Sands Centre Redevelopment		1 April 2019
KD.08/19	The Medium Term Financial Plan (including the Corporate Charging Policy) & the Capital Investment Strategy 2020/21 to 2024/25	22 July 2019 consultation period to include Overview and Scrutiny as appropriate	19 August 2019
KD.09/19	The Asset Management Plan 2019 to 2024	22 July 2019 consultation period to include Scrutiny as appropriate	19 August 2019
KD.10/19	Food Law Enforcement Service Plan 2019/2020	29 May 2019 consultation period to include Overview and Scrutiny as appropriate	17 June 2019
KD.11/19	BIC Project, Paternoster Row, Carlisle		15 April 2019

Notice of Key Decisions to be taken by the Executive

The following key decision is to be made on behalf of Carlisle City Council:

Key Decision Reference:	KD.05/19
Type of Decision:	Executive
Decision Title:	2018/19 Provisional Outturn Reports
Decision to be taken:	The Executive will be asked to consider and approve the 2018/19 Provisional Outturn reports and make recommendations on any carry forward requests to Council on 16th July 2019 • Provisional Revenue Outturn • Provisional Capital Outturn • Elected Members Allowances – Provisional Outturn • Council Tax and National Non-Domestic Rates – Provisional Outturn • Treasury Management Provisional Outturn
Date Decision to be considered:	
Date Decision to be taken:	29 May 2019
Is the Decision Public or Private?:	The decision will be taken in public
Documents submitted for consideration in relation to the Decision:	The report of the Corporate Director of Finance and Resources will be available five working days before the meeting
Contact Officer for this Decision:	Corporate Director of Finance and Resources, Carlisle City Council, Civic Centre, Carlisle, CA3 8QG
Relevant Portfolio Area:	Finance, Governance and Resources (Councillor Dr Tickner)
Relevant or Lead Overview and Scrutiny Panel:	Business and Transformation Scrutiny Panel

All public reports can be viewed in the Customer Contact Centre of the Civic Centre, Carlisle, the Public Library and on the Council's website www.carlisle.gov.uk.

Other documents relevant to the matter may be submitted to the decision maker. These, if available, may be obtained by contacting the named contact officer.

Notice of Key Decisions to be taken by the Executive

The following key decision is to be made on behalf of Carlisle City Council:

Key Decision Reference:	KD.07/19
Type of Decision:	Executive
Decision Title:	Sands Centre Redevelopment
Decision to be taken:	The Executive will be provided with a final design and tender cost for redeveloping the Sands Centre in line with the City Councils Sports Facilities Strategy. Executive will be asked to review these proposals and refer the matter to full Council for approval and any necessary adjustments to the Council's Budget Framework.
Date Decision to be considered:	
Date Decision to be taken:	1 April 2019
Is the Decision Public or Private?:	The decision will be taken in private. The report is not for publication by virtue of paragraph 3 of Part 1 of Schedule 12A of the Local Government Act 1972, as the report contains exempt information relating to the financial or business affairs of any particular person (including the authority holding that information)
Documents submitted for consideration in relation to the Decision:	The report of the Deputy Chief Executive will be available five working days before the meeting
Contact Officer for this Decision:	Deputy Chief Executive, Carlisle City Council, Civic Centre, Carlisle, CA3 8QG
Relevant Portfolio Area:	Culture, Heritage and Leisure (Councillor Ms Quilter)
Relevant or Lead Overview and Scrutiny Panel:	Health & Wellbeing Scrutiny Panel and Business & Transformation Scrutiny Panel

All public reports can be viewed in the Customer Contact Centre of the Civic Centre, Carlisle, the Public Library and on the Council's website www.carlisle.gov.uk.

Other documents relevant to the matter may be submitted to the decision maker. These, if available, may be obtained by contacting the named contact officer.

Notice of Key Decisions to be taken by the Executive

The following key decision is to be made on behalf of Carlisle City Council:

Key Decision Reference:	KD.08/19
Type of Decision:	Executive
Decision Title:	The Medium Term Financial Plan (including the Corporate Charging Policy) & the Capital Investment Strategy 2020/21 to 2024/25
Decision to be taken:	The Executive will be asked to consider the Council's Medium Term Financial Plan and Corporate Charging Policy, and the Council's Capital Investment Strategy and make recommendations to Council on 10th September 2018
Date Decision to be considered:	22 July 2019 consultation period to include Overview and Scrutiny as appropriate
Date Decision to be taken:	19 August 2019
Is the Decision Public or Private?:	The decision will be taken in public
Documents submitted for consideration in relation to the Decision:	The report of the Corporate Director of Finance and Resources will be available five working days before the meeting
Contact Officer for this Decision:	Corporate Director of Finance and Resources, Carlisle City Council, Civic Centre, Carlisle, CA3 8QG
Relevant Portfolio Area:	Finance, Governance and Resources (Councillor Dr Tickner)
Relevant or Lead Overview and Scrutiny Panel:	Business and Transformation Scrutiny Panel

All public reports can be viewed in the Customer Contact Centre of the Civic Centre, Carlisle, the Public Library and on the Council's website www.carlisle.gov.uk.

Other documents relevant to the matter may be submitted to the decision maker. These, if available, may be obtained by contacting the named contact officer.

Notice of Key Decisions to be taken by the Executive

The following key decision is to be made on behalf of Carlisle City Council:

Key Decision Reference:	KD.09/19
Type of Decision:	Executive
Decision Title:	The Asset Management Plan 2019 to 2024
Decision to be taken:	The Executive will be asked to consider the Council's Asset Management Plan and make recommendations to Council on 10 September 2019
Date Decision to be considered:	22 July 2019 consultation period to include Scrutiny as appropriate
Date Decision to be taken:	19 August 2019
Is the Decision Public or Private?:	The decision will be taken in public
Documents submitted for consideration in relation to the Decision:	The report of the Corporate Director of Governance and Regulatory Services will be available five working days before the meeting
Contact Officer for this Decision:	Corporate Director of Governance and Regulatory Services, Carlisle City Council, Civic Centre, Carlisle, CA3 8QG
Relevant Portfolio Area:	Finance, Governance and Resources (Councillor Dr Tickner)
Relevant or Lead Overview and Scrutiny Panel:	Business and Transformation Scrutiny Panel

All public reports can be viewed in the Customer Contact Centre of the Civic Centre, Carlisle, the Public Library and on the Council's website www.carlisle.gov.uk.

Other documents relevant to the matter may be submitted to the decision maker. These, if available, may be obtained by contacting the named contact officer.

Notice of Key Decisions to be taken by the Executive

The following key decision is to be made on behalf of Carlisle City Council:

Key Decision Reference:	KD.10/19
Type of Decision:	Executive
Decision Title:	Food Law Enforcement Service Plan 2019/2020
Decision to be taken:	The Executive will be asked to decide the Regulatory Service's inspection and educational priorities for improving food safety in Carlisle during 2019 /2020.
Date Decision to be considered:	29 May 2019 consultation period to include Overview and Scrutiny as appropriate
Date Decision to be taken:	17 June 2019
Is the Decision Public or Private?:	The decision will be taken in public
Documents submitted for consideration in relation to the Decision:	The report of the Corporate Director of Governance and Regulatory Services will be available five working days before the meeting
Contact Officer for this Decision:	Corporate Director of Governance and Regulatory Services, Carlisle City Council, Civic Centre, Carlisle, CA3 8QG
Relevant Portfolio Area:	Environment and Transport (Councillor Southward)
Relevant or Lead Overview and Scrutiny Panel:	Health and Wellbeing Scrutiny Panel

All public reports can be viewed in the Customer Contact Centre of the Civic Centre, Carlisle, the Public Library and on the Council's website www.carlisle.gov.uk.

Other documents relevant to the matter may be submitted to the decision maker. These, if available, may be obtained by contacting the named contact officer.

Notice of Key Decisions to be taken by the Executive

The following key decision is to be made on behalf of Carlisle City Council:

Key Decision Reference:	KD.11/19
Type of Decision:	Executive
Decision Title:	BIC Project, Paternoster Row, Carlisle
Decision to be taken:	The Executive will be asked to consider the options for the BIC Project
Date Decision to be considered:	
Date Decision to be taken:	15 April 2019
Is the Decision Public or Private?:	The decision will be taken in private. The report is not for publication by virtue of paragraph 3 of Part 1 of Schedule 12A of the Local Government Act 1972, as the report contains exempt information relating to the financial or business affairs of any particular person (including the authority holding that information)
Documents submitted for consideration in relation to the Decision:	The joint report of the Corporate Director of Economic Development and the Corporate Director of Governance and Regulaotry Services will be available five working days before the meeting
Contact Officer for this Decision:	Corporate Director of Economic Development and Corporate Director of Governance and Regulatory Services, Carlisle City Council, Civic Centre, Carlisle, CA3 8QG
Relevant Portfolio Area:	Economy, Enterprise and Housing (Councillor Mrs Glendinning) and Finance, Governance & Resources (Councillor Dr Tickner)
Relevant or Lead Overview and Scrutiny Panel:	Business & Transformation Scrutiny Panel and Economic Growth Scrutiny Panel

All public reports can be viewed in the Customer Contact Centre of the Civic Centre, Carlisle, the Public Library and on the Council's website www.carlisle.gov.uk.

Other documents relevant to the matter may be submitted to the decision maker. These, if available, may be obtained by contacting the named contact officer.

Notice prepared by Councillor Colin Glover,
Leader of Carlisle City Council

Date: 15 March 2019

INDIVIDUAL PORTFOLIO HOLDER DECISIONS

Below is a list of decisions taken by Individual Portfolio Holders acting under delegated powers, full details can be viewed on the Council's website www.carlisle.gov.uk:

PF.001/19 **Sands Centre Extension Project**

Portfolio Holder who made Decision: Councillor Glover

Portfolio Area: Leader

Subject Matter:

The Sands Centre Extension Project is now reaching a critical milestone in its development and the City Council will consider recommendations on this matter on 9th April 2019.
In order to meet the timetable for considering these recommendations the Portfolio Holder has decided to take any reports associated with this project directly to Business and Transformation and the Health and Wellbeing Scrutiny Panels on 26th March 2019 rather than first consider the matter at Executive.

Summary of Options rejected: None

DECISION

To submit the Sands Centre extension project report directly to the Business and Transformation and Health and Wellbeing Scrutiny Panels on 26th March 2019 rather than first at Executive.

Reasons for Decision

To allow the Sands Centre Extension Project report to advance directly to the relevant scrutiny panels before progressing to Executive and City Council for consideration.

Background Papers considered:

N/A

Date Decision Made: 01/03/19 **Implementation Date:** 15-Mar-19

Officer Decisions

Below is a list of decisions taken by Officers of Carlisle City Council which they have classed as significant, full details and supporting background documents can be viewed on the Council's website: http://cmis.carlisle.gov.uk/cmis/CouncilDecisions/OfficerDecisions.aspx

Decision Ref No	Title:	Subject and Decision Taken:	Reports and Background Papers considered:	Date Decision Taken:
Licensing Manager				
OD.017/19	Licensing Decisions taken between 1 February 2019 and 28 February 2019	The Licensing Manager has granted the attached licences or permissions under an express authorisation delegated to her and in accordance with the Council's policy requirements. (can be viewed on the Council website http://CMIS.carlisle.gov.uk/CMIS/CouncilDecisions/OfficerDecisions.asp x)	Applications for various licences	28/02/2019
Neighbourhood Services Manager				
OD.018/19	Contract for opening and closing of barriers in designated car parks	To proceed with the contract to open and close barriers in three designated car parks.	None	07/03/2019
Property Services Manager				
OD.019/19	Landlord's consent to a new letting.	To grant Landlord's consent to the grant of a new lease of unit 55 at the Lanes Shopping Centre.	None	11/03/2019
Corporate Director of Governance and Regulatory Services				
OD.020/19	Appointment of The OT Practice, Unit 3, Meridian Office Park, Osborn Way, Hook, RG27 9HY as contractor for the provision of Occupation Therapy services to the Council for providing assessments under the Disabled Facility Grant process.	A contract is to be issued to the successful contractor for delivering an Occupation Therapy service as part of the disabled adaptation process. The service is offered as an additional option for grant applicants and does not replace the service offer led by Cumbria County Council Adult Social Care Team. This service forms part of the Regulatory Reform Order (Housing Assistance), updated November 2018.	Procurement submissions and legal contracts. Private - Not for Publication by Virtue of Paragraph 3 of Part 1 of Schedule 12A of the Local Government Act.	01/03/2019

Decision Ref No	Title:	Subject and Decision Taken:	Reports and Background Papers considered:	Date Decision Taken:
Corporate Director of Economic Development				
OD.021/19	Endorsement of ACT (ACTion with Communities in Cumbria) as the preferred consultant to deliver the Cumbria and Lancaster Community-Led Housing Hub.	That ACT are appointed as the preferred consultant to deliver the Hub, following a tender on the The Chest, which was assessed by all six local authorities in the Partnership. Executive gave approval for Carlisle to lead on procurement and preparing a legal agreement, as the other partners would be jointly providing £65,000 funding received through the Community Housing Fund.	Executive report ED.38/18 Cumbria and Lancaster Community-Led Housing Hub	25/02/2019
Deputy Chief Executive				
OD.022/19	Acceptance of funding associated with the Cumbria One Public Estate (OPE) Fund Application	To accept £120,000 grant funding from the OPE programme to develop and deliver a Cumbria-wide programme of estate consolidation and development. The District Councils and Cumbria County Council have been working together with other key public sectors partners to engage with the Governments OPE programme. This work yielded an application to the programme in December 2018. The application was recently approved and an award of £120,000 has been made to our partnership to assist with the development of the programme. Carlisle City Council is acting as the lead agency in this programme and as such will manage the use of this grant.		14/03/2019
Corporate Director of Governance and Regulatory Services				
OD.023/19	Appointment of DarntonB3 as contractor for the provision of drawing and technical servics for disabled adaptations.	A contract is to be issued to the successful contractor for delivering an architect service as part of the disabled adaptation process. The contractor will provide architectural services in connection with the disabled facility grants function. This service forms part of the Regulatory Reform Order (Housing Assistance), updated November 2018.	Procurement submissions and legal contracts. Private Not for Publication by Virtue of Paragraph 3 of Part 1 of Schedule 12A of the Local Government Act.	28/08/2018
Deputy Chief Executive				
OD.024/19	European Regional Development Fund: Low Carbon Outline Application	The Decision has been taken to submit an Outline Application (Expression of interest) to the Low Carbon: call in Cumbria – Priority Axis 4: Supporting the Shift Towards A Low Carbon Economy In All Sectors (OC07R18P 0835)	None	13/03/2019

Decision Ref No	Title:	Subject and Decision Taken:	Reports and Background Papers considered:	Date Decision Taken:
Licensing Manager				
OD.025/19	Licensing Decisions taken between 1 March 2019 and 29 March 2019	The Licensing Manager has granted the attached licences or permissions under an express authorisation delegated to her and in accordance with the Council's policy requirements. (can be viewed on the Council website http://CMIS.carlisle.gov.uk/CMIS/CouncilDecisions/OfficerDecisions.asp x)	Applications for various licences	29/03/2019

JOINT MANAGEMENT TEAM

Monday 11th March 2019

MINUTES

Present:	Councillor C Glover (Chair), A Glendinning, C Southward, L Sherriff, L Tickner, A Quilter D Crossley, A Taylor, M Lambert, J Meek, S Robinson, M Walshe
Apologies:	J Gooding

JMT – Minutes of Previous Meeting	**Action**
The minutes of the previous meeting were agreed.	
Delivering of Affordable Housing in Carlisle	**Action**
JM gave an overview of the background to this paper and there was a discussion concerning the options available. It was agreed further data is required.	**JM**
BIC Options Report	
MW and SR provided the background to the site pre-December 2017 and summarised the key options available for consideration. A full report will be brought to Executive 15th April.	
JMT Forward Plan	
The forward plan to be updated.	
Notice of Executive Key Decisions	
The Notice of Executive Key Decisions were agreed.	

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

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.

CARLISLE CITY COUNCIL www.carlisle.gov.uk	**Report to: EXECUTIVE**	**Agenda Item: A.6**

Meeting Date:	15 April 2019
Portfolio:	Finance, Governance and Resources
Key Decision:	No
Within Policy and Budget Framework	Yes
Public / Private	Public

Title:	Regulation of Investigatory Powers: Update
Report of:	Corporate Director of Governance and Regulatory Services
Report Number:	GD.19/19

Purpose / Summary:

The Report updates the Executive on the Council's use of the surveillance powers open to it under the Regulation of Investigatory Powers Act 2000 (RIPA) and suggests updates to the Council's RIPA policy, for approval by the Executive, in the light of revised Home office Guidance (August 2018). The Policy is recommended by the Audit Committee.

Recommendations:

That the Executive:

i. Note and approve the content of the Report;
ii. Approve the revised Policy as appended to the Report.
iii. Delegate authority to the Corporate Director of Governance and Regulatory Services to update the policy both as necessary and/or to implement any recommendations/observations of the Investigatory Powers Commissioner.

Tracking

Executive:	**15 April 2019**
Audit Committee:	**4 March 2019**

1. BACKGROUND

1.1 Members are aware that, when carrying out covert surveillance activity, the Council must comply with the Regulation of Investigatory Powers Act 2000 (RIPA) and its associated Regulations and Guidance.

1.2 RIPA provides for public authorities to give authorisation to carry out covert surveillance activities. The term 'public authorities' includes local authorities, therefore, the Council may authorise its officers to carry out covert surveillance. Any authorisation signed by the Council is subject to further approval by a Justice of the Peace.

1.3 The basic premise of RIPA is to ensure that covert surveillance is carried out in the appropriate manner. It requires that the public body wishing to carry out such surveillance does so after carrying out a balancing exercise in which the need for covert surveillance is balanced against the rights of the individual. Article 8 of the Human Rights Act 1998 provides that there shall be no interference with an individual's right to respect for his private and family life other than is necessary in the interests of, *inter alia*, public safety, the prevention of crime and disorder, the protection of health or morals, or for the protection of the rights and freedoms of others. For covert surveillance to be justified it must be both necessary and proportionate. If it is possible to obtain evidence overtly then this is the method by which it should be gathered.

1.4 Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to surveillance are unaware that it is taking place. Directed Surveillance includes surveillance which is covert (but not intrusive) which is conducted for a specific investigation/operation and is likely to result in the obtaining of private information about a person.

1.5 Although the term surveillance covers a wide range of activities, it is important to note that RIPA applies only to covert surveillance. If the person who is subject to the surveillance is aware that it is taking place it will not be necessary to obtain authorisation under RIPA.

1.6 The purpose of RIPA is to place covert surveillance activities on a lawful footing. The impetus for this has arisen from the coming into force of the Human Rights Act 1998 ("HRA"). If a public authority fails to comply with the HRA it is in breach of statutory duty and two possible consequences may follow:

- any person who has suffered loss due to such breach may claim compensation from the public authority; and/or
- any enforcement proceedings brought by a public authority against a person who has suffered such breach may be subject to "collateral challenge" by way of defence of non-compliance by the public authority with the HRA.

1.7 The HRA brings into English Law Article 8 of the European Convention on Human Rights ("Article 8"). This provides that any person is entitled to respect for his private and family life, his home and his correspondence. A public authority should not act in a way which is incompatible with this right; if it does the consequences set out above may flow.

1.8 However, Article 8 goes on to provide that there shall be no interference by a public authority with the exercise of the Article 8 right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others. It is therefore recognised by the Convention that interference with Article 8 rights may sometimes be necessary in order to prevent crime/disorder, protect health etc, such interference must however be on a lawful basis. For the purposes of RIPA, the Council is only able to exercise the power for the purpose of preventing/detecting crime or of preventing disorder.

1.9 If a Local Authority fails to obtain an authorisation for surveillance in accordance with the scheme set out in the RIPA it has not thereby committed a criminal offence nor is it automatically subject to any sanction or penalty imposed under civil law. However, in the absence of authorisation there is a risk that the Authority will not be able to demonstrate that any covert surveillance has been carried out on a lawful

basis. There then arises the further risk that any proceedings which the Authority is then undertaking against the person concerned (e.g. statutory enforcement proceedings or a prosecution) may be subject to a successful challenge and/or the Authority may be subject to a legal claim for compensation by the person concerned.

1.10 Local authorities in England and Wales can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The offences relating to the latter are in article 7A of the 2010 RIPA Order.

1.11 Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

1.12 Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud (DWP).

1.13 Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted (Cumbria County Council function).

1.14 The Code of Guidance says: “A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.”

2. CARLISLE CITY COUNCIL RIPA USAGE

2.1 The Guidance says that elected members of a local authority should review the usage of the surveillance powers and set the policy once each year. Members will note how restrictive the rules regulating surveillance are and the reality is that, since the transfer of the Council's benefit fraud to the Department for Work and Pensions, it is very unlikely that we will need to undertake any covert surveillance activity. The last authorisation of surveillance by the City Council predated the transfer of the Benefit Fraud Team.

2.2 In effect, the Council does not make use of any covert surveillance in its activity. **The last authorisation was in March 2014 for a benefit fraud matter.**

3. TRAINING

3.1 RIPA training is part of the Ethical Governance Training Programme and, by way of awareness raising, the concept of covert surveillance and its implications is mentioned whenever possible, for example at witness training. In addition, bespoke RIPA training is delivered, with the most recent event taking place in February 2019. Officers from licensing, regulatory services, civil enforcement, waste services and car parking attended and they in turn will raise awareness within their teams.

4. POLICY

4.1 The Home Office released revised guidance both for Directed Surveillance and also the use of Covert Human Intelligence Sources. The links to these documents are as follows or Members should contact the Corporate Director of Governance and Regulatory Services if they would like a hard copy:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

4.2 The Council's policy document has been amended to reflect the revised guidance and is attached as the Appendix to this Report. The Executive is asked to approve the revised Policy as recommended by the Audit Committee.

5. Oversight

5.1 Oversight of the regime is undertaken by the Investigatory Powers Commissioner and they undertake an inspection every three years. They have been made aware that, like many Councils, we do not make use of the available powers to authorise covert surveillance. On this basis, the last inspector was satisfied that the Council would carry out training as and when necessary but the Commissioner required that it be undertaken irrespective of our use of the powers as it is important to dispel any perception that the training led to any undue influence on the recipient thereof.

5.2 The most recent inspection took place on 26 March 2019. The inspection report will be received in four to six weeks' time however, as an interim update, the Inspector advised that we 'were in a very good place' and he was only going to make one recommendation and a small number of observations. The recommendation will be that Authorising Officers receive periodic refresher training.

6. CONSULTATION

6.1 Not applicable.

7. CONCLUSION AND REASONS FOR RECOMMENDATIONS

7.1 The content of the Report should reassure Members that the City Council takes its responsibilities under the RIPA legislation seriously and also that it continues to strive to be one of the better performing local authorities.

8. CONTRIBUTION TO THE CARLISLE PLAN PRIORITIES

8.1 Compliance with RIPA assists the Council in acting lawfully and promoting its enforcement activities in the District.

Contact Officer: Mark Lambert **Ext:** 7019

In compliance with Section 100d of the Local Government (Access to Information) 1985 the report has been prepared in part from the following papers: **The Home Office Guidance documents referred to in the Report.**

CORPORATE IMPLICATIONS:

LEGAL – The report deals with relevant legal implications.

FINANCE – None

EQUALITY – All persons are treated equally under this legislation.

INFORMATION GOVERNANCE – The codes of practice are clear on how information is to be stored, accessed, disseminated, retained and destroyed.

Appendices attached to report: Revised Council RIPA Policy

Appendix to GD.19/19

CARLISLE CITY COUNCIL

REGULATION OF INVESTIGATORY

POWERS ACT 2000

PROTOCOL AND GUIDANCE NOTES

FOR STAFF

RELATING TO SURVEILLANCE

AND USE OF

COVERT HUMAN

INTELLIGENCE SOURCES

IMPORTANT NOTICE

The RIPA Regime is subject to oversight by the Investigatory Powers Commission Office. Advice, guidance and Codes of Practice may be found at:

https://www.ipco.org.uk

RIPA Codes of Practice and Guidance may be found at:

https://www.gov.uk/government/collections/ripa-codes

The Council's RIPA Policy is subordinate to the Codes of Practice.
Internal points of Contact are:

Mark Lambert	RIPA Monitoring Officer
Clare Liddle	Deputy RIPA Monitoring Officer

CONTENTS

SECTION 1

INTRODUCTION

1.1 The Regulation of Investigatory Powers Act (RIPA) 2000 provides for public authorities to give authorisation to carry out **covert surveillance** activities. Public Authorities include local authorities therefore the Council may itself give authorisation (subject to judicial approval) to its officers to carry out covert surveillance.

1.2 The basic premise of RIPA is to ensure that covert surveillance is carried out in the appropriate manner. It requires that the public body wishing to carry out such surveillance does so after carrying out a balancing exercise in which the need for covert surveillance is balanced against the rights of the individual. Article 8 of the Human Rights Act 1998 provides that there shall be no interference with an individual's right to respect for his private and family life other than is necessary in the interests of, inter alia, public safety, the prevention of crime and disorder, the protection of health or morals, or for the protection of the rights and freedoms of others. For covert surveillance to be justified it must be both **necessary** (para 4.2.3) and **proportionate** (para 4.2.5). If it is possible to obtain evidence overtly then this is the method in which it should be gathered.

1.3 Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to surveillance are unaware that it is taking place. The definition of surveillance is very wide and includes such activities as:

- Monitoring, observing or listening to persons, their movements their conversations or their other activities or communication;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by or with the assistance of a surveillance device.

Although the term surveillance covers a wide range of activities, it is important to note that RIPA applies only to covert surveillance. If the person who is subject to the covert surveillance is aware that it is taking place it will not be necessary to obtain authorisations under RIPA.

1.4 The purpose of RIPA is to place covert surveillance activities on a lawful footing. The impetus for this has arisen from the coming into force of the Human Rights Act 1998 ("HRA").

1.5 If a public authority fails to comply with the HRA it is in breach of statutory duty and two possible consequences may follow:

- any person who has suffered loss due to such breach may claim compensation from the public authority; and/or

- any enforcement proceedings brought by a public authority against a person who has suffered such breach may be subject to "collateral challenge" by way of defence of non-compliance by the public authority with the HRA.

1.6 The HRA brings into English Law Article 8 of the European Convention on Human Rights ("Article 8"). This provides that any person is entitled to respect for his private and family life, his home and his correspondence. A public authority should not act in a way which is incompatible with this right; if it does the consequences set out above may flow.

1.7 However, Article 8 goes on to provide that there shall be no interference by a public authority with the exercise of the Article 8 right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others.

It is therefore recognised by the Convention that interference with Article 8 rights may sometimes be necessary in order to prevent crime/disorder, protect health etc., such interference must however be on a lawful basis.

1.8 In anticipation of the coming into force of the HRA it was recognised that covert surveillance activities were in danger of falling foul of Article 8, even if necessary for the reasons set out in Article 8, if it was not demonstrably carried out on a lawful basis.

1.9 RIPA was therefore enacted in order to provide a clear, lawful basis for covert surveillance to be carried out by public authorities including:

- Security Services

- Police
- Armed Forces
- Customs & Excise
- Local Authorities

1.10 RIPA makes it clear that the Council can only authorise use of directed surveillance to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least six months' imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products (note that these alcohol/tobacco/nicotine issues are not ones which the City Council deals with).

1.11 RIPA assists by:

- Clarifying what types of covert surveillance may be undertaken by local authorities;

- Providing a scheme for the giving/obtaining of authorisation.

1.12 If a Local Authority fails to obtain an authorisation for surveillance in accordance with the scheme set out in the RIPA it has not thereby committed a criminal offence nor is it automatically subject to any sanction or penalty imposed under civil law. However, in the absence of authorisation there is a risk that the Authority will not be able to demonstrate that any covert surveillance has been carried out on a lawful basis. There then arises the further risk that any proceedings which the Authority is then undertaking against the person concerned (e.g. statutory enforcement proceedings or a prosecution) may be subject to a successful challenge and/or the Authority may be subject to a legal claim for compensation by the person concerned.

1.13 The City Council has decided that it **does not** carry out any non-RIPA compliant surveillance, however, the Surveillance Commissioner has requested that this reference to such surveillance be included in this Policy. If such surveillance was conducted it would not have the protection of RIPA as explained in 1.12. To minimise this risk an internal authorisation procedure should be used utilising the forms, rules and guidance applicable to a normal RIPA compliant authorisation process. The fact that the Commissioner has requested that this information be included in the Policy is not to be taken as any indication that the decision stated in the first sentence of this paragraph has been weakened or diluted. **We do not carry out such surveillance.**

1.13 In order to provide public authorities with guidance the Home Office has issued various Codes of Guidance. Those which apply to local authorities and therefore to

Carlisle City Council are as follows (with cross reference to the relevant appendix to this protocol in brackets):

- Covert Surveillance Code of Practice (Appendix 2) – this contains guidance on Directed Surveillance at Chapter 3;

- Covert Human Intelligence Sources Code of Practice (Appendix 3).

1.14 The Government has published a range of information (including the aforementioned codes) on the internet and the Investigatory Powers Commissioner's Office also publishes helpful information at: https://www.ipco.org.uk/ .

1.15 The purposes of this protocol document is to explain what the Council's procedures are for the authorisation and carrying out of Directed Surveillance and the use of Covert Human Intelligence Sources and also to provide guidance for staff who are designated as Authorising Officers or who are authorised to carry out Directed Surveillance or to use or act as Covert Human Intelligence Sources.

1.16 This protocol document sets out the key concepts which are used in the Act. An understanding of such key concepts is essential for all officers who are designated as Authorising Officers or who are authorised to carry out covert surveillance or who are authorised to use or act as Covert Human Intelligence Sources. It also sets out the procedures for obtaining authorisations and the Council's requirements for record keeping.

1.17 This protocol does not purport to be an authoritative interpretation of the law and is in no way intended to be read in substitution for the RIPA, the Regulations and the Codes of Practice. In the event of any doubt, legal advice should be obtained from the RIPA Monitoring Officer (Corporate Director of Governance and Regulatory Services) or Deputy RIPA Monitoring Officer (Legal Services Manager).

1.18 Authorising Officers are responsible for ensuring that staff who report to them follow this Policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document. Authorising Officers must also acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and ensure compliance with the same.

1.19 The RIPA Monitoring Officer is responsible for maintaining a centralised record of all authorisations issued by the Council for the carrying out of Directed Surveillance and for the use of Covert Human Intelligence Sources. The records include not only the

authorisations themselves but also information relating to reviews, renewals and cancellations.

1.20 It is the responsibility of each Directorate to retain a copy of the authorisations, renewals and cancellations in its own centralised file. A copy should be placed on the individual case file and the original sent to the RIPA Monitoring Officer marked "Confidential".

1.21 Authorisation, Renewal and Cancellation forms are available on request from the RIPA Monitoring Officer or in his absence the Deputy RIPA Monitoring Officer. Forms will be obtained from the Home Office website to ensure that the most up to date forms are used. A link to the relevant forms is provided in Appendix 5.

SECTION 2

WHAT IS AUTHORISED UNDER RIPA?

2.1 This Section of the protocol sets out in very brief terms what is and what is not authorised for Local Authorities under RIPA.

2.2 The words and concepts which are used are defined in Section 3 of this Protocol and reference should be made to that Section in order to obtain a full understanding of the terms used.

2.3 The Council may undertake **"directed surveillance"** if it is properly authorised in accordance with the Act.

2.4 The Council **does not** have any power to authorise the carrying out of **intrusive surveillance**. This can only be authorised by high ranking Police Officers, Customs Officers, Officers of the Armed Forces or the Secretary of State. It is highly unlikely that the Council would ever have the need to undertake intrusive surveillance; only the Secretary of State could authorise the Council to do so. However, as a word of caution, the Council must take care not to carry out intrusive surveillance inadvertently.

2.5 The Council is also empowered under the RIPA to use "**Covert Human Intelligence Sources"**.

2.6 The Council is not empowered to enter on and interfere with property and wireless telegraphy (although some types of public bodies are authorised to do so under the RIPA).

2.7 Authorisations to carry out such surveillance may be given in public authorities by "Authorising Officers". Regulations issued under RIPA provide that the only persons who are entitled to act as Authorising Officers in local authorities are officers at Director, Head of Service, Service Manager or equivalent (see the **Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010/521**).

2.8 Appendix 4 sets out the current Authorising Officers.

SECTION 3

DIRECTED SURVEILLANCE
AND
COVERT USE OF HUMAN INTELLIGENCE SOURCE

3.1 This part of the Protocol describes the concepts of:

- Directed Surveillance;
- Covert Human Intelligence Source.

These terms are used in Part II of RIPA and the Codes.

3.2 **What is "Directed Surveillance"?**

Surveillance is "directed surveillance" if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining pf private information about a person (whether one specifically identified for the purpose of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought.

3.2.1 *What is "Surveillance"?*

Under RIPA this is defined to mean:

"(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device."

RIPA states that surveillance does not include:

(a) any conduct of a Covert Human Intelligence Source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source; (For example, if you confront a neighbour with evidence obtained by a professional witness or tenant in an attempt to shame them into better behaviour);

(b) the use of a Covert Human Intelligence Source for so obtaining or recording information, or any entry on or interference with property or wireless telegraphy as this would be unlawful unless authorised under warrants for the intelligence service legislation or powers of police and customs officers.

3.2.2 *Is the surveillance covert?*

Surveillance is covert if and only if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

Whether or not the surveillance is covert is the first question which should be asked when considering the seeking of authorisation; if it is not covert, the framework of the RIPA will not apply. **Overt surveillance should be used whenever possible (paras 4.2.4 and 4.2.5).**

3.2.3 *Is it for the purposes of a specific investigation or a specific operation?*

This may include, for example, an investigation into a complaint relating to anti-social behaviour in relation to the occupants of particular premises, or a complaint relating to noise arising from specific premises or an anti-fraud operation conducted in relation to Housing/Council Tax Benefits.

3.2.4 *Is it in such a manner that is likely to result in the obtaining of private information about a person?*

“Private information" is any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. As a result, private information is capable of including any aspect of a person’s private or personal relationship with others, such as family and professional or business relationships.

Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts etc.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities may still result in the obtaining of private information. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

3.2.5 *Online covert activity*

The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

As set out in the next paragraph, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.2.6 *Is the Surveillance Intrusive?*

Directed surveillance becomes Intrusive Surveillance if it:

- is carried out in relation to anything taking place on residential premises, or
- is in any private vehicle, and
- involves the presence of an individual on the premises or in the vehicle, or
- is carried out by means of a surveillance device.

Furthermore, surveillance is intrusive if it is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

If the device is not on the premises or in the vehicle, it is only Intrusive Surveillance if it consistently produces information of the same quality as if it were. This might catch sound recording equipment which is placed in premises next door to the premises which is under investigation.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

THE COUNCIL IS <u>NOT</u> AUTHORISED TO CARRY OUT INTRUSIVE SURVEILLANCE.

3.3 **Covert use of Human Intelligence Source (CHIS – also known as a "source")**

A person is a source if:

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph

(b) or (c) below;

(b) he covertly uses such a relationship to obtain information or provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Thus, a source may include persons such as agents, informants and officers working undercover.

3.3.1 *Covert purpose*

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

3.3.2 *Covertly uses such a relationship*

A relationship is used covertly, and information obtained as mentioned in 3.4.1(c) above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties is unaware of the use or disclosure in question.

3.3.3 Note that an informant, even if not tasked by the Council to obtain information on its behalf, would nevertheless fall within the definition of a CHIS if s/he has obtained the relevant information in the course of, or as the result of the existence of, a personal or other relationship, such as that of friend, relative or acquaintance. In other words, it is 'inside information' as opposed to information obtained through outside observation. In this scenario, it is unlikely that a CHIS authorisation is required but a duty of care is owed to the informed as regards how and whether the information may be safely used. It is best to seek advice from the RIPA Monitoring Officer if there is any doubt.

3.3.4 *Information*

It is not clear from the Act whether "information" means only "private information". The inference is there, but it is not expressly stated in the RIPA.

3.4 Activity not falling within the definition of covert surveillance

3.4.1 Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance authorisation can be obtained for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;

- covert surveillance not relating to the statutory grounds specified in the 2000 Act;

- overt use of CCTV systems

Immediate response

3.4.2 Covert surveillance that is likely to reveal private information about a person, but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under the 2000 Act, would not require a directed surveillance authorisation. The 2000 Act is not intended to prevent law enforcement officers fulfilling their legislative functions. To this end, section 26(2)(c) of the 2000 Act provides that surveillance is not directed surveillance when it is carried out by way of an immediate response to events or circumstances, the nature of which is such that it is not reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

General observation activities

3.4.3 The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

Surveillance not relating to specified grounds or core functions

3.4.4 An authorisation for directed or intrusive surveillance is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation is necessary on the grounds specified in the 2000 Act (specified at section 28(3) for directed surveillance and at section 32(3) for intrusive surveillance). Covert surveillance for any other general purposes should be conducted under other legislation, if relevant, and an authorisation under Part II of the 2000 Act should not be sought.

3.4.5 The ‘core functions’ referred to by the Investigatory Powers Tribunal are the ‘specific public functions’, undertaken by a particular public authority, in contrast to the ‘ordinary functions’ which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.). These “ordinary functions” are covered by the Data Protection Act 2018 and the Information Commissioner’s Employment Practices Code. A public authority may only seek authorisations under the 2000 Act when in performance of its ‘core functions’. For example, the disciplining of an employee is not a ‘core function’, although related criminal investigations may be. As a result, the protection afforded by an authorisation under the 2000 Act may be available in relation to associated criminal investigations, so long as the activity is deemed to be necessary and proportionate.

Overt surveillance cameras

3.4.6 The use of overt CCTV cameras by public authorities does not normally require an authorisation under the 2000 Act. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly

visible, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner. Public authorities should also be aware of the relevant Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information").

3.4.7 The Surveillance Camera code has relevance to overt surveillance camera systems (as defined at s29(6) of the 2012 Act) and which are operated in public places by relevant authorities (defined at s 33(5) of the 2012 Act) in England and Wales. The 2012 Act places a statutory responsibility upon those public authorities defined by the 2012 Act, to have regard to the provisions of the Surveillance Camera code, where surveillance is conducted overtly by means of a surveillance camera system in a public place in England and Wales.

3.4.8 The Surveillance Camera code sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 2018 and a public authority's duty to adhere to the Human Rights Act 1998. **The City Council has its own CCTV surveillance camera policy**.

3.4.9 However, where overt CCTV or other overt surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or other overt surveillance cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

SECTION 4

AUTHORISATIONS, RENEWALS AND DURATION ETC

4.1 How is authorisation obtained?

4.1.1 As stated above, authorisation may be given by Authorising Officers for:

- Directed Surveillance;
- Covert Use of Human Intelligence Sources.

4.1.2 The Council is only able to authorise the use of Directed Surveillance to prevent or detect criminal offences that are punishable by a maximum term of **at least** 6 months' imprisonment or are related to the sale of underage sale of alcohol or tobacco.

4.1.3 The Council is no longer able to authorise directed surveillance for the purposes of preventing disorder (unless punishable by a maximum term of at least six months' imprisonment). It is possible to authorise directed surveillance for 'serious' cases as long as the usual tests of necessity and proportionality are met. Examples would be more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. The guidance from the Home Office says, "A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low level offences which may include, for example, littering, dog control and fly-posting". To authorise directed surveillance, the Authorising Officer must demonstrate that the proposed activity is necessary for the prevention or detection of a crime which either carries a maximum sentence of at least six months' imprisonment or is an offence relating to the sale of alcohol or tobacco products to minors (see RIPA, s81(5) for the definition of "detecting crime").

4.1.4 At the commencement of investigations, officers will need to satisfy themselves that what they are investigating is a criminal offence etc. If, during the investigation, the likely offence is graded downwards, below the six month imprisonment threshold, then any RIPA authorisation should be cancelled.

4.1.5 It is important to bear in mind that for offences which no longer meet the relevant threshold that routine patrols, observations at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

4.1.6 The person seeking an Authorisation should complete the relevant Authorisation form which should be obtained from the RIPA Monitoring Officer or his/her Deputy. A link to the relevant forms is provided in Appendix 5. Having completed the form he should then take it to the Authorising Officer. In order to provide as full information as possible to enable the Authorising Officer to make a fully informed decision, detailed information should be given in the forms regarding "necessary" and "proportionality" (see below).

4.1.7 The Authorising Officer must take the following steps when considering whether or not to give an Authorisation:

- consider if Authorisation is necessary

- Consider if what will be carried out is proportionate to what is sought to be achieved by carrying it out;

- Is there sufficient information in the form? Has it been completed correctly? What must be recorded in the application form in respect of Directed Surveillance is explained at paragraph 4.2.7 below, and in the case of Covert Use of Human Intelligence Sources in paragraph 4.3.2 below;

- Consider potential for collateral intrusion, the steps that may be taken to minimise it and whether a separate authorisation is required. This is explained in paragraphs 4.2.6, 4.2.8 and 4.3.6 below; in the case of Use of a Covert Human Intelligence Source consider arrangements for safety and welfare of the source; before authorisation, a risk assessment should be undertaken - see paragraph 4.3.5;

- Consider any adverse impact on community confidence that might flow from the authorisation. Sensibilities in the local community should be considered where the surveillance is taking place; consider also activities being undertaken by other public authorities which could impact upon the deployment of surveillance; consider the circumstances where the subject of the surveillance might expect a high degree of privacy (eg in the home or where there are special sensitivities).

4.1.8 **Related authorisations:** if the action authorised refers to activity under a previous authorisation, the Unique Reference Number (URN) and details of that authorisation to enable cross reference to be done. The Authorising Officer should ensure that there is no conflict with previous or other current authorisations.

4.1.9 If the Authorising Officer is satisfied that Authorisation should be given, he should obtain the reference number from the RIPA Monitoring Officer. He should then sign the form, record the date and time that the Authorisation is given, and endorse the reference number on the form. He should send the original of the form to the RIPA Monitoring Officer (who is responsible for maintaining the Central Register for the whole Council) in a sealed envelope marked "Confidential", keep a copy in his own Department's central file of Authorisations and place a copy on the case file.

4.1.10 In addition, from 1 November 2012, the Protection of Freedoms Act 2012, sections 37 & 38 apply. The effect of this is that the Council still has to authorise Directed Surveillance (when it is available) in the usual manner but any authorisation (or application for renewal) **has to be secondly approved by a Justice of the Peace**. The Authority will have to make an appointment with the Magistrates' Court office; supply the Court with a copy of the RIPA form together with a cover application form and then attend a hearing at which, hopefully, the JP will approve the authorisation. JP approval will also be necessary for any renewal of an authorisation.

4.1.11 The Guidance says that any applications before the Magistrates are deemed 'legal proceedings' and that presenting officers should be authorised under section 223 of the Local Government Act 1972 to appear on behalf of the Council. Appropriate authorisations may be obtained from the RIPA Monitoring Officer. Appointments with the Justices of the Peace are made via the Carlisle Magistrates' Court Office.

4.2 The Conditions for Authorisation - Directed Surveillance

4.2.1 For Directed Surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

(a) that an authorisation is necessary (on the ground detailed below); and

(b) the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

4.2.2 An authorisation is **necessary** if it is for the purpose of preventing or detecting crime or of preventing disorder;

4.2.3 Significant consideration must be given to the issue of **necessity**. Everyone has the right to respect for his private and family life (Article 8, Human Rights Act 1998). There shall be no interference with this right other than is necessary in the interests of, inter alia, public safety, the prevention of crime and disorder, the protection of health or morals, or for the protection of the rights and freedoms of others. "Necessity" has to be established on the facts of each individual case before an individual's rights of privacy can be legitimately infringed. Consideration must be given as to why it is necessary to use covert surveillance in the investigation.

4.2.4 Section 80 of RIPA provides a general saving for lawful conduct, i.e. if the conduct in question does not require authorisation under the Act and is lawful in any event then it continues to be lawful. The effect of this section is that if the Council's duty can be carried out without recourse to an authorisation then that is the preferred way to do it. In other words, if the required information can be obtained by overt means in any given circumstance, covert surveillance can never be necessary. The authorisation forms contain a section in which the applicant is required to identify why covert surveillance is necessary in any given case. **It is the task of the authorising officer to apply his mind to this, as well as proportionality, before granting an authorisation.**

4.2.5 In addition, the authorisation for the activity must be **proportionate**. This involves a balancing exercise of the need for the activity in operational terms against the degree of interference with the rights of the subject of the surveillance and of any other persons. It will not be proportionate if the interference is excessive in the circumstances of the case or if the information could have been obtained using less intrusive means. All activity must be carefully managed and must not be arbitrary or unfair. When assessing proportionality, consideration must be given to whether the proposed covert surveillance is proportional:

a) To the mischief being investigated;
b) To the degree of likely intrusion on the target and others; and
c) Whether other reasonable means of obtaining the evidence have been considered and discounted.

4.2.6 The onus is therefore on the **Authorising Officer** who is considering an application to authorise such surveillance to be satisfied that it is:

(a) necessary for the ground stated above and;

(b) is proportionate to its aim.

4.2.6 The Home Office Code of Practice (August 2018)[1] states that a potential model application would make clear that the following elements of proportionality had been fully considered:

a. Balancing the size and scope of the operation against the gravity and extent of the perceived mischief.
b. Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others.
c. Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought.
d. Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

4.2.7 The **conduct** that is authorised by an authorisation is any conduct which

(a) consists of the carrying out of Directed Surveillance of any such description as is specified in the authorisation; and

(b) is carried out in the circumstances specified in the authorisation and for the purposes of the investigation or operation specified or described in the authorisation.

It therefore follows that if Directed Surveillance that is actually conducted is other

[1] Para 4.7

than that specified in the authorisation and/or is carried out in circumstances other than those so specified, and/or for a purpose other than that so specified, it will be unauthorised and unlawful. Careful thought should therefore be given when framing an application for authorisation as to the:

- scope of the directed surveillance;

- the circumstances in which it shall be conducted;

- the purpose of the investigation.

The wider the scope of this authorisation the easier it will be to demonstrate that the activities fell within it. On the other hand, it should not be drafted so widely as to be meaningless! The scope of an authorisation should not be widened on a "just in case" basis.

It is also sensible to make any authorisation sufficiently wide enough to cover all the measures required as well as being able to prove effective monitoring of what is done against what is authorised.

4.2.8 Consideration should be given as to whether there is any possibility that **collateral intrusion** may occur. Collateral intrusion is when the privacy of persons who are other than the subject/s of the investigation/operation is impinged upon. Wherever possible steps should be taken to minimise interference in the lives of persons who are not subject(s) of the investigation. An application for authorisation should therefore include an assessment of the risk of collateral intrusion. If anticipated, the potential for intrusion of this type should be minimised. The ongoing possibility for collateral intrusion should be monitored by the Authorising Officer, such monitoring should form part of the continuing review process to which authorisations are subject. The potential for collateral intrusion may be significant enough to warrant refusal of the application for authorisation. If, during the course of an investigation/operation, the privacy of persons other than the subjects of the investigation/operation are unexpectedly interfered with, this should be reported to the Authorising Officer and he should consider whether the original authorisation should be amended or whether a separate authorisation is required.

4.2.9 **Collateral intrusion** is perhaps the most important aspect of proportionality because it constitutes an invasion of the privacy of persons who are not the target of the surveillance who may not be connected in any way to the ongoing investigation and are probably entirely innocent.

4.2.10 Authorisations shall be given in **writing** by the Authorising Officer. Authorising Officers should not generally be responsible for authorising their own activities but exceptionally this might be unavoidable.

4.2.11 Written application for a directed surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and on which statutory ground(s) (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;

- the nature of the surveillance;

- the identities, where known, of those to be the subject of the surveillance;

- a summary of the intelligence case and appropriate unique intelligence references where applicable;

- an explanation of the information which it is desired to obtain as a result of the surveillance;

- the details of any potential collateral intrusion and why the intrusion is justified;

- the details of any confidential or privileged information that is likely to be obtained as a consequence of the surveillance;

- where the purpose, or one of the purposes, of the authorisation is to obtain information subject to legal privilege[43], an assessment of why there are exceptional and compelling circumstances that make this necessary;

- the reasons why the surveillance is considered proportionate to what it seeks to achieve; and

- the level of authorisation required (or recommended where that is different) for the surveillance.

- applications should avoid any repetition of information;

- information contained in applications should be limited to that required by the relevant legislation and the requirements of this code;

- the case for the warrant or authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which support or weakens the case for the warrant or authorisation;

- an application should not require the sanction of any person in a public authority other than the authorising officer;

- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the application;

- authorisations or warrants should not generally be sought for activities already authorised following an application by the same or a different public authority.

and subsequently record whether authority was given or refused, by whom and the time and date.

4.2.12 Code of Practice Guidance for the Council

The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisations subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorisation from a judicial authority, before it can take effect. In England and Wales an application for such an order must be made to a Justice of the Peace (JP). If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he or she will issue an order approving the grant or renewal for the use of the technique as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 has the following effect.

- The Council can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The offences relating to the latter are in article 7A of the 2010 RIPA Order.

- The Council **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

- The Council may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more are ones involving more serious criminal damage or dangerous waste dumping.

- The Council may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted. In Carlisle, this type of offence is dealt with by the County Council.

- The Council **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

- Within the Council, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Investigatory Powers Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed. Carlisle City Council's senior responsible officer is the Corporate Director of Governance and Regulatory Services.

- Elected members of the Council should review the authority's use of the 1997 Act and the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 1997 Act and the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

YOU ARE RECOMMENDED TO SEEK ADVICE FROM THE LEGAL SERVICES UNIT WHEN CONSIDERING ANY APPLICATION FOR A CHIS AUTHORISATION OR ANY MATTER RELATED THERETO

4.3 **Conditions for Authorisation - Covert Use of Human Intelligence Sources**

4.3.1 The Authorising Officer must be satisfied that the use of a Covert Human Intelligence Source is necessary and proportionate. In these respects the principles set out in paragraph 4.2 should be applied. Authorisations should be given in writing and Authorising Officers should not be responsible for authorising their own activities eg acting as source or tasking a source save exceptionally where this would otherwise be unavoidable. **Note that the same secondary authorisation process by a Justice of the Peace, both for initial authorisations and their renewal, apply to CHIS** (see 4.1.10 and 4.1.11).

4.3.2 An application for the use or conduct of a source should record:

- details of the purpose for which the source will be tasked or deployed (e.g. in relation to anti-social behaviour);

- the grounds on which authorisation is sought (eg for the purpose of preventing or detecting crime or preventing disorder);

- where a specific investigation or operation is involved, details of that investigation or operation;

- details of what the source will be tasked to do;

- details of the level of authority required (or recommended, where that is different);

- details of potential collateral intrusion;

- details of any confidential material that might be obtained as a consequence of the authorisation.

4.3.3 The conduct so authorised is any conduct that:

(a) is comprised in any such activities involving conduct of a Covert Human Intelligence Source, or the use of a Covert Human Intelligence Source, as are specified or described in the authorisation;

(b) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a Covert Human Intelligence Source the authorisation relates; and

(c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

4.3.4 Nothing in the 2000 Act prevents material obtained from the use or conduct of the source being used in evidence in Court proceedings. Existing Court discretion and procedures can protect, where appropriate, the disclosure of the source's identity.

4.3.5 The Authorising Officer must consider the safety and welfare of that source, and the foreseeable consequences to others of the tasks they are asked to carry out. A **risk assessment** should be carried out before authorisation is given. Consideration for the safety and welfare of the source, even after cancellation of the authorisation, should also be considered.

4.3.6 Before authorising the use or conduct of a source, the Authorising officer should believe that the conduct/use including the likely degree of **intrusion** into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation ("collateral intrusion": for an explanation as to the meaning of this reference should be made to paragraph 4.2.8 above). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

4.4 Record Keeping in relation to Sources

4.4.1 Accurate and proper recording keeping should be kept about the source and tasks undertaken although the confidentiality of the source must be maintained. Records of all authorisations should be maintained on the Central Register of Authorisations referred to in Section 5 of this Protocol which should contain the following information:

- the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- the reason why the person renewing an authorisation considered it necessary to do so;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the Authorising Officer to cease using a source.

These records shall be retained for a period of at least 3 years from the ending of the authorisation.

RIPA provides that an Authorising Officer must not grant an authorisation for the conduct or use of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

4.4.2 Records should be kept not only of the Authorisation but of the use of the source as well. The records should contain particulars of:

(a) the identity of the source;

(b) the identity or identities used by the source, where known;

(c) the means used within the Council of referring to the source;

(d) any other significant information connected with the security and welfare of the source;

(e) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in (d) has been considered and that any identified risks to the security and welfare of the source have been properly explained to and understood by the source;

(f) the date when and circumstances in which the source was recruited;

(g) where applicable, the relevant investigating authority in relation to the source (other than the authority that is maintaining the records);

(h) the identities of the persons in the relevant investigating authority who, in relation to the source, are discharging or have discharged the responsibilities

mentioned in paragraph 4.5.2 of this Protocol where relevant;

(i) the period for which those responsibilities have been discharged by those persons;

(j) the tasks that are given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of the Council;

(l) the information obtained by the Council by the conduct or use of the source;

(m) the information so obtained which is disseminated by the Council;

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward or every offer of a payment, benefit or reward that is made or provided by or on behalf of the Council in respect of the source's activities for the benefit of the Council.

4.4.3 The records must be maintained in such a way so as to preserve the anonymity of the source and the information provided by the source. The RIPA Monitoring Officer shall be responsible for maintaining the Central Register of Authorisations which will include the information referred to in paragraph 4.4.1 relating to Authorisations and the Authorising Officer shall maintain the information referred to in paragraph 4.4.2 above relating to the use of the source.

4.5 **Management and Tasking of Sources**

4.5.1 The Authorising Officer must ensure that satisfactory arrangements exist for the management of the source and for bringing to his attention any concerns about the personal circumstances of the source in so far as they might affect:

- the validity of the risk assessment;
- the proper conduct of the source operation, and
- the safety and welfare of the source.

Where such information is brought to the attention of the Authorising Officer, he shall determine whether or not the authorisation shall continue.

4.5.2 RIPA requires that the Council in common with other public authorities; ensures that arrangements are in place for the proper management and oversight of sources including:

- an Officer of the Council will have responsibility for dealing with the source on behalf of the Council ("the Dealing Officer"): this person will usually be below the grade of Authorising Officer;

- another Officer shall have general oversight of the use made of the source ("the Oversight Officer").

4.5.3 The Dealing Officer will have day to day responsibility for:

- dealing with the source on behalf of the Council;
- directing the day to day activities of the source;
- recording the information applied by the source; and,
- monitoring the source's security and welfare.

4.5.4. It will always be sensible to give careful consideration to the scope of tasking of the source. Whenever it becomes apparent to the Dealing Officer or the Oversight Officer that unforeseen action has taken place or where it is intended to task the source in a new or significantly greater way, they must refer the proposed tasking to the Authorising Officer who will consider whether a separate authorisation is required.

4.5.5 Whenever the Council deploys a source it should take into account the safety and welfare of the source when carrying out the action which he has been tasked to do. As stated at paragraph 4.3.5 above, before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment has been carried out. The Dealing Officer is responsible for bringing to the attention of the Oversight Officer any concerns about the personal circumstances of the source including the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate these concerns should be considered by the Authorising Officer who will decide whether or not to allow the authorisation to continue.

4.6 **Limits of Source's Authority**

A source may, in the context of an authorised operation, infiltrate existing criminal activity, or be a party to the commission of criminal offences, within the limits recognised by law. A source who acts beyond these limits will be at risk of prosecution. The need to protect the source cannot alter this principle.

4.7 **Cultivation of a source**

4.7.1 Cultivation is the process of developing a relationship with a potential source, with the intention of:

- Covertly making a judgement as to his/her likely value as a source of information;
- Covertly determining whether and, if so, the best way in which to propose to the subject that he/she become a source.

4.7.2 It may be necessary to infringe the personal privacy of the potential source in the process of cultivation. In such cases, authorisation is needed for the cultivation process itself, as constituting the conduct (by the person undertaking the cultivation) of a source.

4.8 Use and conduct of a source

Authorisation for the use and conduct of a source is required prior to any tasking. Tasking is an assignment given to the source, asking him or her to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. It may involve the source infiltrating existing criminal activity in order to obtain that information.

4.9 Vulnerable individuals

Vulnerable individuals should only be authorised to act as source in the most exceptional circumstances. The meaning of the term Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or unable to protect himself against significant harm or exploitation. Only the Chief Executive or in his absence, a Chief Officer may grant an Authorisation for the use of a vulnerable individual.

4.10 Juvenile sources

4.10.1 Special safeguards also apply to the authorisation for the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his or her parents. In other cases, authorisations should not be granted unless:

- A risk assessment has been undertaken as part of the application to deploy a juvenile source, covering the danger of physical injury and the psychological aspects (eg distress) of his or her deployment;

- The risk assessment has been considered by the authorising officer and he has satisfied himself that any risk identified in it have been properly explained and understood, by the source; and

- The authorising officer has given particular consideration as to whether the juvenile is to be tasked to get information from a relative, guardian or any other person who has for the time being assumed responsibility for his welfare and whether the authorisation is justified in the light of that fact.

4.10.2 In addition, juvenile authorisations should not be granted unless the Authorising Officer believes that arrangements exist which will ensure that there will at all times be a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between the authority and a source under 16 years of age. An "Appropriate Adult" is the parent or guardian of the source; any other

person who has assumed responsibility for his welfare or in the absence of any of the foregoing any responsible person aged 18 or over who is not a member of nor employed by the Council.

4.10.3 The duration of an Authorisation is **one month** instead of 12 months.

4.10.4 Only the Chief Executive or in his absence a Chief Officer may grant an Authorisation of the use of a juvenile.

4.11 Not used.

4.12 **Confidential Material**

4.12.1 RIPA does not provide any special protection for 'confidential material'. Briefly "confidential material" has a special meaning under RIPA and comprise any of the following:

- communications subject to legal privilege;
- confidential personal information;
- confidential journalistic material;

For a further explanation of these terms please refer to the definitions section in Appendix 1.

Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the Home Office codes. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of Confidential Material, the deployment of the source should be subject to special authorisation by the Head of the Paid Service (Town Clerk and Chief Executive) or (in his/her absence) a Chief Officer. Careful attention should be paid to the provisions in the Home Office codes (Chapter 3 of the Covert Surveillance Code of Practice and Chapter 3 of the Covert Human Intelligence sources Code of Practice).

4.12.2 In general, any application for an authorisation which is likely to result in the acquisition of Confidential Material should include an assessment of how likely it is that Confidential Material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling Confidential Material. Such applications should only be made in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

4.12.3 The following general principles apply to Confidential Material acquired under Part II authorisations:

- Those handling material from such operations should be alert to anything which may fall within the definition of Confidential Material. Where there is doubt as to whether the material is confidential, advice should be sought from the RIPA Monitoring Officer before further dissemination takes place;

- Furthermore, careful regard should be had to the provisions in the Home Office Codes of Practice relating to confidential material referred to above.

- Confidential Material should not be retained or copied unless it is necessary for a specified purpose;

- Confidential Material should be disseminated only where an appropriate officer (having sought advice from a legal officer) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

- Confidential Material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

4.13 **Combined authorisations - joint working etc**

4.13.1 In cases of joint working i.e. with other agencies on the same operation, authority for directed surveillance by the Council's Officers must be obtained from the Council's Authorising Officers. Authority cannot be granted by the Benefit Authority's Authorising Officers for the actions of Council staff and vice versa.

4.13.2 The above paragraph refers to joint operations where the Council is working on the same operation as a partner agency. However, it is also possible for one organisation to act as 'principal' and one as 'agent' (i.e. the 'agent' is not necessarily carrying out the activities as part of its own operations). The 'principal' organisation will issue the authorisation and ensure that the agent is fully aware of the precise terms of the surveillance to be carried out, thus ensuring that the limits imposed by the authorisation on invasion of privacy are observed. If no collaboration agreement exists between the parties it is wise for the arrangement to be recorded in writing and the 'agent' should acknowledge that they act in the said capacity and will comply with the authorisation.

4.13.2 Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the Use of a Covert Human Intelligence Source.

4.14 **Duration/Renewals**

4.14.1 Authorisations lapse, if not renewed:

- within 72 hours if either granted or renewed orally, (or by a person whose authorisation was confined to urgent cases) beginning with the time of the last grant or renewal, or

- 12 months - if in writing/non-urgent - from date of last renewal if it is for the conduct or use of a Covert Human Intelligence Source (Juvenile CHIS authorisation = one month) or

- in all other cases (ie Directed Surveillance) 3 months from the date of their grant or latest renewal.

4.14.2 An authorisation can be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms. (See paragraph 4.15.4 below)

However, for the conduct of a Covert Human Intelligence Source, a person should not renew unless a review has been carried out and that person has considered the results of the review when deciding to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

4.14.3 Regular reviews should be carried out of all authorisations which have been issued: it is for the Authorising Officer to determine the frequency of reviews to be carried out. Once a review has been conducted the result should be notified in writing to the RIPA Monitoring Officer in order that it may be recorded on the Central Register. In the case of CHIS authorisations, the review should include the use made of the source, the tasks given to the source and the information obtained from the source. In particular, reviews should be carried out frequently when it is likely that confidential material may be obtained or collateral intrusion may take place.

4.14.4 An authorisation may be reviewed, renewed, before it is due to expire, and such renewal for up to a further 3 months (Directed Surveillance or, 12 months CHIS) if the Authorising Officer considers this to be necessary. An application for renewal, in the case of Directed Surveillance should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

- any significant changes to the information in paragraph 4.2.8 (Directed Surveillance) or 4.3.2 (CHIS);

- the reasons why it is necessary to continue with the Directed Surveillance/use of the source;

- the content and value to the investigation or operation of the information so far obtained by the surveillance;

- in the case of a CHIS the use made of the source since the date of the authorisation/renewal the tasks given to him and the information obtained from him;

- the results of regular reviews of the investigation or operation.

Authorisations may be renewed more than once, if necessary, and the renewal

should be kept/recorded as part of the central record of authorisations. Note that it is necessary to obtain the approval of a Justice of the Peace for any renewal.

4.15 **Cancellations**

The Authorising Officer has a statutory duty to cancel an authorisation once satisfied that the criteria for authorisation of Directed Surveillance or the use or conduct of a source (as appropriate) are no longer satisfied (s45 RIPA). If the Authorising Officer is no longer available, the task will fall on the person who has taken over the role of Authorising Officer. Cancellations shall contain the information and Authorising Officer Directions in accordance with the Code of Practice.

4.16 **Retention and destruction of product**

4.16.1 Authorising Officers are reminded of the guidance relating to the retention and destruction of Confidential Material as described in paragraph 4.12 above.

4.16.2 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after Directed Surveillance activity is no longer necessary.

4.16.3 Authorising Officers must ensure that copies of each authorisation are sent to the RIPA Monitoring Officer as described in Section 5 below.

4.16.4 Authorisations for Directed Surveillance or CHIS are to be securely retained by the Authorising Officer, for a period of 3 years from the ending of the Authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, in accordance with established disclosure requirements (e.g. Civil Procedure Rules; Code of Practice under the Criminal Procedures and Investigations Act (1996)) commensurate to any subsequent review. Once the investigation is closed (bearing in mind cases may be lodged sometime after the initial work) the records held by the Directorate should be disposed of in an appropriate manner (e.g. shredded).

4.16.5 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by Directed Surveillance or through use of a CHIS which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.16.6 There is nothing in the RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the authority which authorised the surveillance, or the courts, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

SECTION 5

CENTRAL REGISTER OF AUTHORISATIONS

AND RETENTION REQUIREMENTS

5.1. The Council has a Statutory Monitoring Officer who also fulfils the responsibility of the Council's RIPA Monitoring Officer. As such, the RIPA Monitoring Officer is responsible for the oversight of the Council's RIPA activities, the maintenance of the RIPA Protocol, maintenance of the Central Register of Authorisations. The RIPA Monitoring Officer will ensure that all involved have the appropriate level of training. He or she provides definitive advice for the purposes of RIPA and officers should not hesitate to seek assistance if required. In the absence of the RIPA Monitoring Officer the Deputy Monitoring Officer will also act as Deputy RIPA Monitoring Officer.

5.2 The RIPA requires a central register of all authorisations to be maintained by authorities coming within the Act. The Council's RIPA Monitoring Officer maintains this register. The following information shall be centrally retrievable for a period of at least three years:

- the type of authorisation/warrant;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation (if applicable);
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- for local authorities, details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- the dates of any reviews;

- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;

- whether the authorised activity is likely to result in obtaining confidential or privileged information as defined in this code of practice[67];

- whether the authorisation was granted by an individual directly involved in the investigation;

- the date the authorisation was cancelled;

- where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;

- a record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner;

- where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

The following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the authorising officer;
- for local authorities a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace (JP).

5.3 Whenever an authorisation is issued (including renewals and when cancellations are issued) the Authorising Officer must forthwith arrange for a the fully detailed Authorisation (including the JP authorisation) to be sent to the RIPA Monitoring Officer in a sealed envelope marked “Confidential” and to his Directorate’s Record holder, with a further copy being placed on the individual case file.

5.4 In addition, the following documentation should be retained, by the Record Holder in the Directorates where authorisation has taken place:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer and the Justice of the Peace;

- a record of the period over which the investigation/surveillance has taken place;

- the frequency of reviews prescribed by the Authorising Officer;

- a record of the result of each review of the authorisation;

- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- the date and time when any instruction was given by the Authorising Officer.

- a copy of any cancellation of the authorisation.

5.5 The RIPA Monitoring Officer or his nominated deputy shall be responsible on a monthly basis for reviewing any outstanding authorisations contained within the Central Register. In particular, the RIPA Monitoring Officer should ascertain whether authorisations have been reviewed or cancelled as appropriate by the relevant Authorising Officer.

5.6 The RIPA Monitoring Officer should signify that the required monthly review has been satisfactorily conducted by signifying to this effect on the review log contained within the Central Register of Authorisations.

SECTION 6

CODES OF PRACTICE

6.1 There are Home Office codes of practice that expand on this guidance and copies are available on the Home Office website or on request from Legal Services.

6.2 The codes do not have the force of statute but are admissible in evidence in any criminal and civil proceedings. The 2000 Act provides that all codes of practice issued under the Act are admissible as evidence in criminal and civil proceedings. Any court or tribunal considering such proceedings, the Investigatory Powers Tribunal , or the Investigatory Powers Commissioner responsible for overseeing the relevant powers and functions, may take the provisions of the codes of practice into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

6.3 Staff should refer to the Home Office Codes of Practice via the links in the relevant appendices:-

- Covert Surveillance Code of Practice (Appendix 2) – this contains guidance on Directed Surveillance at Chapter 3;
- Covert Human Intelligence Sources Code of Practice (Appendix 3).

6.4 The front page of this Policy also provides a link to the Investigatory Powers Commissioner's Office website which provides guidance and procedures.

SECTION 7

BENEFITS OF OBTAINING AUTHORISATION UNDER THE 2000 ACT.

7.1 Authorisation of surveillance and human intelligence sources

The RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and
- the conduct is in accordance with the authorisation, then
- it shall be “lawful for all purposes”.

However, the corollary is not true – i.e. if you do not obtain the RIPA authorisation it does not automatically make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). However, you cannot take advantage of any of the special RIPA benefits and that may entail that any enforcement action taken by the Council following unauthorised conduct may be subject to collateral challenge under the Human Rights Act 1998. Furthermore, if a person can prove that their Article 8 rights have been infringed as a result of unauthorised conduct they may sue the Council and claim compensation.

7.2 The RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which -

(a) is incidental to any conduct that is lawful by virtue of S27(1); and

(b) is not itself conduct an authorisation or warrant for which is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

SECTION 8

SCRUTINY AND TRIBUNAL

8.1 To effectively "police" RIPA, there is provision for the setting up of Commissioners to provide independent oversight carried out thereunder. It provides for the appointment of a Chief Surveillance Commissioner to keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, of the powers and duties in Part II. This includes authorising Directed Surveillance and the use of Covert Human Intelligence Sources.

8.2 RIPA also provides for the establishment of a tribunal to consider and determine complaints made under the RIPA. It will be made up of senior members of the legal profession or judiciary and shall be independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

Complaints can be made by persons aggrieved by conduct e.g. Directed Surveillance. The forum hears applications on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among others, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation or records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if

- It has granted any authorisations under Part II of the 2000 Act.
- It has engaged in any conduct as a result of the authorisation.
- We hold the rank, office and position in a public authority for whose benefit any such authorisation has been or may be given.

APPENDIX 1

Definitions from the 2000 Act

- "1997 Act" means the Police Act 1997.
  "2000 Act" means the Regulation of Investigatory Powers Act 2000.

- **"Confidential Material"** has the same meaning as it is given in sections 98-100 of the 1997 Act.

  It consists of:

  (a) matters subject to legal privilege;

  (b) confidential personal information; or

  (c) confidential journalistic material.

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below)

- **"Confidential Personal Information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  (a) to his/her physical or mental health; or

  (b) to spiritual counselling or other assistance given or to be given, and

  which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office (see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

  (c) it is held subject to an express or implied undertaking to hold it in confidence; or

  (d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- "**Confidential Journalistic Material"** includes material acquired or created

for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

- "**Covert Surveillance"** means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

- For the purposes of authorising directed surveillance under the 2000 Act an "authorising officer" means the person designated for the purposes of section 28 of the 2000 Act to grant authorisations for directed surveillance.

- **"Working Day"** means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom

Note A. *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.*

Note B. *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

APPENDIX 2

COVERT SURVEILLANCE

CODES OF PRACTICE

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

APPENDIX 3

COVERT HUMAN INTELLIGENCE SOURCES

CODE OF PRACTICE

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

APPENDIX 4

LIST OF AUTHORISING OFFICERS

Corporate Director of Finance and Resources	Alison Taylor
Deputy Chief Executive	Darren Crossley
Development Manager	Christopher Hardman
Regulatory Services Manager	Scott Burns
Town Clerk and Chief Executive (Juvenile or Vulnerable Person CHIS or the acquisition of confidential information.)	Jason Gooding

APPENDIX 5

AUTHORISATION FORMS

All forms may be found from the following link:

https://www.gov.uk/government/collections/ripa-forms--2

Note: Carlisle best practice is to obtain the relevant form direct from the RIPA Monitoring Officer to ensure (a) it is the most up to date form and (b) a URN may be allocated.

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

AUC.09/19 REGULATION OF INVESTIGATORY POWERS: UPDATE

The Corporate Director of Governance and Regulatory Services submitted report GD.16/19 updating the Audit Committee on the Council's use of the surveillance powers open to it under the Regulation of Investigatory Powers Act 2000 (RIPA).

He outlined the background to the matter, reminding Members that the basic premise of RIPA was to ensure that covert surveillance was carried out in the appropriate manner, the justification being that it must be both necessary and proportionate.

The rules regulating surveillance were restrictive and it was, since the transfer of the Council's benefit fraud to the Department of Works and Pensions, unlikely that the Council would need to undertake any covert surveillance activity. The last authorisation for covert surveillance had been in March 2014.

The Corporate Director of Governance and Regulatory Services advised that oversight of the regime was undertaken by the Investigatory Powers Commissioner, with an inspection every three years. They had been made aware that, like many Councils, Carlisle did not make use of the available powers to authorise covert surveillance. On that basis, the last inspector had been satisfied that the Council would carry out training as and when necessary. However, the Commissioner required that it be undertaken irrespective of the Council's use of the powers as it was important to dispel any perception that the training led to any undue influence on the recipient thereof. As a result RIPA training had been included in the Ethical Governance Training Programme and bespoke RIPA training had also been delivered. The next inspection was scheduled for 26 March 2019.

In response to the Committee's questions the Corporate Director of Governance and Regulatory Services confirmed that the protocol captured safeguarding requirements. Regarding surveillance he explained that surveillance carried out by mobile units was advertised in the area and therefore it was overt surveillance outwith the RIPA requirements.

RESOLVED – That the Audit Committee:

1. Noted and approved the content of Report GD.16/19.
2. Recommended the revised Policy to the Executive for approval.
3. Recommended that the Executive delegate authority to the Corporate Director of Governance and Regulatory Services to update the policy both as necessary and/or to implement any recommendations of the Investigatory Powers Commissioner.