

EXECUTIVE MEMBER - THE MAYOR

Date: Tuesday, 17 December 2024
Time: 3.30 p.m.
Venue: Spencer Room, Town Hall

AGENDA

1. Welcome and Fire Evacuation Procedure

In the event the fire alarm sounds, attendees will be advised to evacuate the building via the nearest fire exit and assemble at the Bottle of Notes opposite MIMA.

- | | |
|----------------------------------|---------|
| 2. Business Continuity Policy | 3 - 16 |
| 3. Partnership Governance Policy | 17 - 30 |
| 4. Surveillance Policy 2024/2025 | 31 - 66 |

Charlotte Benjamin
Director of Legal and Governance Services

Town Hall
Middlesbrough
Monday, 9 December 2024

MEMBERSHIP

Mayor C Cooke (Chair)

Assistance in accessing information

Should you have any queries on accessing the Agenda and associated information please contact Chris Lunn, 01642 729742, chris_lunn@middlesbrough.gov.uk

This page is intentionally left blank

MIDDLESBROUGH COUNCIL	
------------------------------	--

Report of:	Director of Legal and Governance Services
-------------------	---

Submitted to:	Individual Executive Member Decision-Making: The Mayor
----------------------	--

Date:	17 December 2024
--------------	------------------

Title:	Business Continuity Policy
---------------	----------------------------

Report for:	Decision
--------------------	----------

Status:	Public
----------------	--------

Strategic priority:	All
----------------------------	-----

Key decision:	No
----------------------	----

Why:	Decision does not reach the threshold to be a key decision
-------------	--

Subject to call in?	Yes
----------------------------	-----

Why:	Not urgent
-------------	------------

Proposed decision(s)
<p>That the Mayor:</p> <ul style="list-style-type: none"> • AGREES the annual review of the Business Continuity Policy.

Executive summary
<p>The Business Continuity Policy sets out how the Council will comply with The Civil Contingencies Act 2004 placed a statutory duty on the council as a designated Category 1 responder to ensure that it can; respond to an emergency, continue to support emergency response partners and continue to provide critical services to the public.</p>

1. Purpose

1.1 The purpose of this report is to set out the Business Continuity Policy which is in place to ensure the Council conducts its statutory duties as an Category 1 responder under The Civil Contingencies Act 2004.

2 Recommendations

2.1 That the Mayor:

- **AGREES** the Business Continuity Policy.

3 Rationale for the recommended decision(s)

3.1 The policy will ensure that there is a consistent framework in place that sets out the council's approach to business continuity.

4 Background and relevant information

4.1 During an emergency or incident Middlesbrough Council is still required to deliver its critical services. Heavy snow, power outage or cyber-attacks are a few examples on how services could be affected, and Service Areas need to maintain plans to ensure they can continue to operate the most essential aspects, even if they lose essential resources. This could be social care being able to reach isolated communities, highways winter maintenance operating with reduced fleet or ICT maintaining computer systems to prevent loss.

4.2 The Council is required to ensure that a policy is in place to govern Business Continuity as part of steps to ensure it meets its legal obligations. Adherence to the policy will ensure compliance with The Civil Contingencies Act 2004. The Act places a statutory duty on Local Authorities as a Category 1 responder to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable. The duty relates to all functions, not just their emergency response functions:

- Emergency management/civil protection: Functions that underpin the Category 1 responder's capability to respond to the emergency itself, and take effective action to reduce, control or mitigate the effects of the emergency.
- Impact on human welfare, the environment and security: The significance of services to the effective functioning of the community in the event of an emergency, or an adverse effect on the environment.
- Legal implications: Statutory requirements on Category 1 responders and the threat of litigation if a service is not delivered or is delivered inadequately.
- Financial implications: Loss of revenue and payment of compensation.
- Reputation: Functions that impact on the credibility and public perception of a Category 1 responder.

4.3 The Risk and H&S team is tasked with ensuring that all MBC directorates and service areas have robust arrangements in place to ensure they are able to deal with a variety

of impacts capable of disrupting their provision of service to the communities of Middlesbrough.

4.4 The business continuity arrangements have evolved to ensure that directorates have plans in place to mitigate and manage disruptive incidents such as a loss of staff, buildings, equipment or disruption to information technology or supply chains. Service Areas create a critical function plan to manage the loss of these resource procedures.

4.5 The Risk and H&S Team continue to consider internal audit with a review of the Councils Business Continuity Plans due in Q4 of this fiscal year 2024/25.

4.6 Compliance with Business Continuity good practice is reported to Audit Committee on an annual basis. Going forward the report will set out compliance with the proposed policy.

5. Other potential alternative(s) and why these have not been recommended

5.1 The Council could choose not to have a policy in place to set out expected standards for its Business Continuity arrangements, however this would increase the risk that the Council could have insufficient arrangements in place to maximise their ability to deliver improved outcomes for the residents of Middlesbrough.

6. Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	There are no direct legal implications as a result of this report.
Legal	There are no direct legal implications as a result of this report. The report supports compliance with the statutory duties placed upon the Council by the Civil Contingencies Act 2004.
Risk	<p>The revised policy impacts positively on the following risks managed within the Legal and Governance Services Directorate Risk Register:</p> <ul style="list-style-type: none"> ● O8-037 - If business continuity plans are not fit for purpose then in the event a business interruption the Council would potentially be unable to provide critical services which could result in harm to service users and a breach of law namely the Civil Contingencies Act 2004. ● O8-052 - Risk of disruption to service delivery, Due to: Lack of adequately tested Business Continuity / Disaster Recovery Plans which fail to effectively manage a critical incident (e.g. relating to access to critical systems / data) and further extend the period of system unavailability. Resulting In: extended or permanent loss of

	systems/data, poor communication and the inability to identify and inform key officers about incident /implications. Failure to reinstate services/systems within an appropriate timescale, dissatisfaction/loss of confidence with the Council's customers.
Human Rights, Public Sector Equality Duty and Community Cohesion	While the policy is not directly relevant to these impact areas, having a policy in place will ensure the Council is better placed to be able to continue to deliver its critical activities and ensure continued compliance with legislation associated with these areas.
Climate Change / Environmental	
Children and Young People Cared for by the Authority and Care Leavers	
Data Protection	

Actions to be taken to implement the recommended decision(s)

6.8 Publication of this policy on the Council’s Internal Data site.

Appendices


1	Business Continuity Policy
----------	----------------------------

Background papers

Reporting body	Report title	Date
Audit Committee	Business Continuity annual assurance report	20231214

Contact:

Gary Welch, Strategic Risk and Health and Safety Manager
Gary_Welch@middlesbrough.gov.uk

	<h2>Business Continuity Policy</h2>
---	-------------------------------------

Creator	Author(s)	Gary Welch - Strategic Risk and Health and Safety Manager		
	Approved by	Executive		
	Department	Legal and Governance Services		
	Service area	Governance Policy & Information		
	Head of Service	Ann-Marie Johnstone - Head of Governance, Policy & Information		
	Director	Charlotte Benjamin - Legal and Governance Services		
Date	Created	02/04/2024		
	Submitted	11/10/2024		
	Approved	Xx/xx/2024		
	Updating Frequency	3 years		
Status	Version: 0.1			
Contributor(s)	Strategic Risk and Health and Safety Manager, Head of Governance, Policy and Information, Risk and Business Continuity Business Partner			
Subject	Middlesbrough Council's policy on managing Business Continuity within the Local Authority			
Type	Policy			
	Vital Record		EIR	
Coverage	Middlesbrough Council			
Language	English			

Document Control

Version	Date	Revision History	Reviser
0.1	20240402	Initial draft	Gary Welch

Distribution List

Version	Date	Name/Service area	Action
1.0	Xx/12/2024	LMT / Intranet	Implement

Contact:	Gary_welch@middlesbrough.gov.uk
-----------------	--



SUMMARY

1. This policy is part of the corporate governance policy framework underpinning the Council plan which:
 - affirms the council's commitment to effective information governance in order to meet all legal obligations, deliver its strategic objectives and to maintain public trust
 - ensures that all information assets are systematically well-managed through the life cycle; and
 - ensures all staff understand their information governance responsibilities.
2. The Business Continuity sets out how the Council will ensure that it can continue to deliver its critical functions when there is an event which could disrupt its usual service delivery.

CONTEXT

3. This should be read alongside the Council's Information Governance Framework and the Risk and Opportunities Management Policy.

PURPOSE

4. The aim of the policy is:
 - Set out how the Council will to anticipate risks, mitigate where possible to reduce the likelihood of its services being interrupted;
 - The plans it will put in place to manage service interruptions; and
 - the maintenance and testing of those plans to ensure they remain fit for purpose.

SCOPE

5. Middlesbrough Council is committed to ensuring robust and effective business continuity management as a key mechanism to restore and deliver continuity of key services in the event of a disruption or emergency.
6. The Civil Contingencies Act 2004 placed a statutory duty on the council as a designated Category 1 responder to ensure that it can:
 - respond to an emergency.
 - continue to support emergency response partners.
 - continue to provide critical services to the public.
7. This policy applies to all directly delivered Council services and ensures a plan is in place for all functions that are deemed to be critical, using the following definition:
 - The Critical Functions Plan are business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the Council's assets, meet Council needs, and satisfy regulations.

8. Commissioned or outsourced services delivering critical functions are required to ensure appropriate business continuity arrangements are in place.

DEFINITIONS

Civil Contingencies Act	The Act which requires that the Council has in place plans for its critical functions to ensure they can continue to be delivered during an emergency.
Business Continuity	Business continuity is an organisation’s ability to maintain or quickly resume acceptance levels of product or service delivery following a short-term event that disrupts normal operations. e.g of disruptions range from natural disasters to power outages.
Critical function	Critical Functions are business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the Council’s assets, meet Council needs, and satisfy regulations.
Business continuity disruption	An event that interrupts normal business functions, operations, or processes whether anticipated or unanticipated
Business Continuity Policy	A business continuity policy is the set of standards and guidelines for Middlesbrough Council to enforces to ensure resilience and good risk management.
Business Continuity Management	A process that helps to identify and plan against risks which could affect the delivery and operation of the council’s priorities and objectives, infrastructure, targets, and areas of public safety for which it is responsible. In the short term the objective of BCM is to ensure that during any disruption critical functions may continue uninterrupted at an acceptable level of performance. In the longer term the objective of BCM is to ensure a full resumption of all normal services as quickly as possible following the disruption.

<p>ISO 22301</p>	<p>The recognised international Business Continuity Standard and within this BC is defined as “the capability of the organisation to continue delivery of products or services at acceptable predefined levels following an incident”. The Good Practice Guidelines 2024 cover all elements of the Standard considering the WHAT, WHY, HOW and WHEN.</p> <p>The BC Standard ISO 22301 highlights 6 key components which form the structure of the Business Continuity Management Programme, and these are referred to as the BCM Lifecycle:</p> <ul style="list-style-type: none"> ▪ Policy & Programme Management. ▪ Embedding BC. ▪ Analysis. ▪ Design. ▪ Implementation. ▪ Validation
<p>Incident management</p>	<p>How the Council will manage any significant disruption to its services, using the Business Continuity Policy and supporting plans.</p>

POLICY DETAIL

9. The Business Continuity Policy is underpinned by a confidential suite of Business Continuity plans that provide the operational structure for responding to serious disruption, and can be summarised as follows:

- Corporate Business Continuity Plan
- Relocation Plan
- Fuel BC Plan
- Pandemic BC Plan
- ICT Disaster Recovery Plan
- Directorate BC Plans

Roles and Responsibilities

10. In order to meet the objectives of this policy it is essential that officers and members are fully conversant with their own roles and responsibilities:

<p>The Mayor and Executive and Elected Members</p>	<ul style="list-style-type: none"> • Overall responsibility for effective management, including agreeing and adherence to the Council’s Business Continuity Policy.
<p>Chief Executive</p>	<ul style="list-style-type: none"> • Responsibility for embedding both the BC Policy and BCM throughout the Council.

	<ul style="list-style-type: none"> • Lead the management of an incident if a Business Continuity event is declared, or delegate responsibility to a member of the Leadership Team.
Leadership Management Team	<ul style="list-style-type: none"> • Receive updates about the BCM Programme • Receive reports on key strategic issues, including as part of the annual statement of assurance, to ensure that Corporate BC risks are being managed • Give robust consideration to the BCM risks contained within reports to committee as part of the decision-making process • Play a part in the management of an incident if appropriate
Executive Directors and Directors	<ul style="list-style-type: none"> • Overall responsibility for embedding the BC Programme across their directorate • Adopt and implement the BC Policy and BCM Framework • Contribute towards the management and review of strategic and cross cutting critical functions of the Council • Receive and consider reports on key strategic BC issues • Promote the integration of BCM principles into the culture of the Council through heads of service • Identify business continuity co-ordinators in their respective directorates and inform the strategic risk and health and safety manager of them • Play a role in the management of an incident if appropriate.
Heads of Service and Service Managers	<p>Heads of Service</p> <ul style="list-style-type: none"> • Ensure that appropriate contingency plans are maintained and reviewed for all council business activities within their area • Provide assurance on the effectiveness of controls in place to mitigate / disruptions within their service via participation in audits and the implementation of audit recommendations • Maintain awareness of and promote the approved BCM Policy and strategy to all relevant staff • Undertake the role of Business Continuity lead during an incident affecting their service area • Play a role in the management of an incident if appropriate <p>Service Managers</p> <ul style="list-style-type: none"> • Review, analyse and profile service critical functions • Prepare, maintain, and review BC Plans for their area of responsibility in liaison with the Corporate BC Group • Third party suppliers should be requested for ongoing assurance that their business continuity arrangements can continue to be relied upon. • Ensure BC is a regular item on team meetings • Maintain awareness of and promote the approved BC Policy and Strategy to all relevant staff • Ensure that BCM considerations which are relevant to their service are incorporated into service plans • Play a role in the management of an incident if appropriate
Corporate BCM Group	<ul style="list-style-type: none"> • Actively promote BC throughout the council • Attend necessary training / exercising in BCM to remain fully competent and aware of current developments

	<ul style="list-style-type: none"> • Be the directorate point of contact for BC issues and co-ordinate activity and communications in the event of an incident (Directorate BC Co-ordinators) • Play a role in the management of an incident if appropriate
<p>Head of Service Governance, Policy and Information</p>	<p>Ensure that:</p> <ul style="list-style-type: none"> • BC documentation is maintained and reviewed • Advice is provided to Leadership team and Executive on BC • Promote a culture of BC awareness within the organisation • BC plans are tested • Report on BC preparedness to Audit Committee on an annual basis • Play a role in the management of an incident if appropriate
<p>Risk and Health and Safety Manager</p>	<ul style="list-style-type: none"> • Act as a deputy to the Head of Service Governance, Policy and Information • Review with plan owners bi-annually all critical function plans. • Review bi-annually all Corporate BC documentation and submit to Head of Service Governance, Policy and Information for authorisation. • Ensure advice is provided to Leadership team and Executive on BC • Promote a culture of BC awareness within the organisation • Ensure that BC plans are tested • Report on BC preparedness to Audit Committee on an annual basis • Play a role in the management of an incident if appropriate • Providing advice and assistance throughout the Business Continuity Programme • Developing appropriate templates for Middlesbrough Council to detail its arrangements, ensuring consistency in the Programme with flexibility to recognise the differences across departments • Supporting departments in completing the documentation from a Business Impact Analysis (BIA) to developing a Critical Function Plan (CFP) • Assisting in the development of wider plans/arrangements to support team DR plans • Raising the profile of Business Continuity across the Council as an ongoing responsibility and ensuring that information is available to staff. • Providing training to appropriate staff and leading on the development of exercises to review arrangements that have been put in place • Reviewing the Programme to ensure it remains fit for purpose and to continuously improve the arrangements in place
<p>Plan Owners</p>	<ul style="list-style-type: none"> • Manage assigned critical function plan from director. • Review critical function plan if any of the following are applicable: <ul style="list-style-type: none"> - If there are changes to the organisation's structure or services. - If there are changes to the environment in which the authority operates.

	<ul style="list-style-type: none"> - Following lessons learned from an incident or exercise. - Following a review or audit. - Following good practice.
All employees	<ul style="list-style-type: none"> • Familiarise themselves with the BCM process • Play a role in the management of an incident if appropriate

Legislative and regulatory framework

11. Key elements of the legislative and regulatory framework relevant to risk management are set out below:

Civil Contingencies Act 2004	Requires the Council to have risk arrangements in place to manage the risk of emergencies occurring and impacting on the public.
Local Government Act 1999	General requirement to achieve value for money. The effective management of risk and opportunity reduces unnecessary expenditure and increases the likelihood of delivering organisational priorities.

Testing and storage of underpinning Business Continuity Plans

12. A business continuity plan cannot be considered reliable until it is exercised and has proved to be workable. There is a continual need to prove plans and strategies by testing them.

13. The authority will exercise its BCM arrangements to ensure that they meet business requirements and are consistent with the business continuity objectives. The authority shall:

- Develop exercises that are consistent with the scope of the objectives.
- Rehearse key staff and those involved in prioritised services.
- Have an exercise programme to ensure exercises are carried out at planned intervals and when significant changes occur.
- Carry out a range of different exercises including tabletop discussions, scenario, simulation, and live exercises that taken together validate the whole of its business continuity arrangements.
- Plan exercises so that the risk of an incident occurring as a direct result of the exercise is minimised.
- Define the aims and objectives of every exercise.
- Carry out a post-exercise review of each exercise that will assess the achievement of the aims and objectives of the exercise.
- Produce a written report of the exercise, including lessons learnt, to determine any amendments required when the plan(s) are updated.

14. The Leadership Management Team will test business continuity arrangements at least annually to ensure credible recovery preparedness.

15. Copies of the BC Plans will be internally saved electronically under secure conditions.

16. Copies will also be held on the Middlesbrough Council's Resilience Direct page which can be accessed by the plan owners.

MONITORING AND REVIEW

17. The Council's expectations around business continuity management are clearly set out within its corporate values and associated competency frameworks. All managers and employees are required to comply with this Business Continuity policy to ensure that the Council effectively manages critical functions to enable its strategic objectives. Managers and employees will be provided with a range of resources, and where appropriate, training, to support the effective implementation of this policy.

18. A maintenance programme will ensure that plans are updated by the plan owner biannually or if there is a significant change in business operations which stems from any of the following:

- As employees or responsibilities change.
- If there are changes to the organisation's structure or services.
- If there are changes to the environment in which the authority operates.
- Following lessons learned from an incident or exercise.
- Following a review or audit.
- Following good practice.

19. An annual assurance report on the Council's business continuity management arrangements will be submitted to Audit Committee.

20. The SIRO or Strategic Risk and Health and Safety Manager will provide quarterly updates to the Council's Risk Management Group around business continuity management.

21. The implementation and effectiveness of this policy and its supporting procedures will be reviewed on a quarterly basis, using the following metrics:

- Accuracy of corporate business continuity plans.
- Management of directorate business continuity plans
- Availability of critical function plans.
- Availability of battle box information.
- Completion rate of training tracking for plan owners.

22. This policy will be reviewed every three years, unless there is significant development that would require a more urgent review e.g., new legislation.

EVALUATION

23. Validation, training, awareness and exercising BCM arrangements and BC plans should be reviewed, exercised, and validated at regular intervals to determine whether any changes are required to procedures and responsibilities.

24. The review should be documented and ensure that the BCM arrangements:

- Accurately reflect the Council's objectives.
- Include a programme for training, exercising and awareness.
- Identify all prioritised service areas and supporting resources.
- Incorporate improvements identified during incidents and exercises.

25. The Council will conduct annual reviews of its Business Continuity Plans and will learn lessons from testing of plans to ensure the effectiveness of this policy and underpinning plans can be evaluated.

This page is intentionally left blank

MIDDLESBROUGH COUNCIL	
------------------------------	--

Report of:	Director of Legal and Governance Services
-------------------	---

Submitted to:	Individual Executive Member Decision-Making: The Mayor
----------------------	--

Date: TBC	17 December 2024
------------------	------------------

Title:	Partnership Governance Policy
---------------	-------------------------------

Report for:	Decision
--------------------	----------

Status:	Public
----------------	--------

Strategic priority:	All
----------------------------	-----

Key decision:	No
----------------------	----

Why:	Decision does not reach the threshold to be a key decision
-------------	--

Subject to call in?	Yes
----------------------------	-----

Why:	Not urgent
-------------	------------

Proposed decision(s)	
That the Mayor: <ul style="list-style-type: none"> • AGREES the Partnership Governance Policy. 	

Executive summary	
The revised Partnership Governance Policy sets out how the Council will ensure a good governance approach to its strategic partnerships.	

1. Purpose

1.1 The purpose of this report is to set out the revised Partnership Governance Policy which is in place to ensure appropriate governance arrangements are in place for the Council’s key strategic partnerships.

2 Recommendations

2.1 That the Mayor:

- **AGREES** the Partnership Governance Policy.

3 Rationale for the recommended decision(s)

3.1 The policy will ensure that there is a consistent framework in place that assesses the health of partnerships governance to ensure the council is able to take appropriate action to maximise the effectiveness of its partnerships.

4 Background and relevant information

4.1 The purpose of a policy for Partnership Governance is to ensure that the Council’s partnerships are managed in line with the principles of good governance, to ensure that the Council works effectively with its partners to maximise its ability to achieve the objectives set out in the Council Plan and demonstrate how the Council meets the requirements of the Best Value Duty. An Effective approach to Partnerships and Community Engagement is one of the seven Best Value themes:



4.2 The policy, appended to this report, sets out that the health of all partnerships will be assessed using the CIPFA ‘Delivering Good Governance in Local Government’ guidance as a framework to assess the following broad principles:

- Whether the partnership behaves with integrity, demonstrating a strong commitment

- to ethical values and the rule of law
- How the partnership ensures compliance with the principles of openness and comprehensive stakeholder engagement
- Defining outcomes in terms of sustainable economic, social and environmental benefits
- Determining the interventions necessary to optimize the achievement of the intended outcomes
- Developing the partnership’s capacity, including the capability of its leadership and the individuals within it
- Managing risks and performance through robust internal control and strong public financial management
- Implementing good practices in transparency, reporting and audit to deliver effective accountability.

4.3 It sets out an expectation that where there is a strategic partnership in place, it should have the following elements within its governance where they are applicable:

- A clear statement on aims and purpose, legal status and obligations
- Targets, objectives and outcomes and that they should be accompanied by milestones
- Risks to the effectiveness of the partnership should be recorded and monitored
- Documented decision making and accountability rules that align with the agreed remit of the partnership and the council’s constitution
- Documented meetings schedule and nominated deputies
- Clear and transparent financial and resourcing arrangements for finances and staffing resources
- Dispute resolution procedures and exit strategy
- An annual review of the partnership through the updating of the Partnership governance register which includes a health assessment
- Alignment with the Council’s minimum standards for programme and projects where the Council is the lead partner
- An assessment completed on an annual basis of the health of the partnership.

4.4 Compliance with this policy is reported to Audit Committee on an annual basis.

5. Other potential alternative(s) and why these have not been recommended

5.1 The Council could choose not to have policy framework document in place to set out expected standards for its partnerships, however this would increase the risk that the Council could have partnerships which do not have the necessary arrangements in place to maximise their ability to deliver improved outcomes for the residents of Middlesbrough.

6. Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	There are no direct financial implications with respect to the approval of this policy.

Legal	There are no direct legal implications as a result of this report. The report supports compliance with the statutory duties placed upon the Council by the Civil Contingencies Act 2004
Risk	<p>The revised policy impacts positively on the following risks within the Strategic Risk Register:</p> <ul style="list-style-type: none"> • If the Council’s Corporate Governance arrangements are not fit for purpose and appropriate action is not taken to rectify this at pace, this could result, censure from the Council’s auditors within a public interest report that would damage the Council’s reputation and/or in government formal intervention including removal of powers from officers and members and direction of council spend. • If the Council and its partners do not have the collective capacity to deliver system wide change to key issues such as public health, crime and safeguarding, then this could result in the population’s health, wellbeing and safety declining.
Human Rights, Public Sector Equality Duty and Community Cohesion	The proposed policy is not directly relevant to these themes however it will enable the Council to have an appropriate governance structure in place to ensure it complies with relevant legislation on this matter, within a partnership setting.
Climate Change / Environmental	The proposed policy is not directly relevant to these themes however it will enable the Council to have an appropriate governance structure in place to ensure it complies with relevant legislation on this matter, within a partnership setting.
Children and Young People Cared for by the Authority and Care Leavers	The proposed policy is not directly relevant to these themes however it will enable the Council to have an appropriate governance structure in place to ensure it complies with relevant legislation on this matter, within a partnership setting.
Data Protection	The proposed policy is not directly relevant to these themes however it will enable the Council to have an appropriate governance structure in place to ensure it complies with relevant legislation on this matter, within a partnership setting.

Actions to be taken to implement the recommended decision(s)

6.8 Publication of this policy on the Council’s Open Data site.

Appendices

1	Partnership Governance Policy
---	-------------------------------

Background papers

Reporting body	Report title	Date
Executive	Delivering the Strategic Plan	20200204
Audit Committee	Partnership Governance annual assurance report	20220929
Audit Committee	Partnership Governance annual assurance report	20231214

Contact:

Ann-Marie Johnstone, Head of Governance, Policy and Information
Ann-marie_johnstone@middlesbrough.gov.uk

This page is intentionally left blank



Partnership Governance Policy

Creator	Author(s)	Ann-Marie Johnstone, Head of Governance, Policy and Information (SIRO)		
	Approved by	Executive		
	Department	Legal and Governance Services		
	Service area	Governance, Policy and Information		
	Head of Service	Ann-Marie Johnstone		
	Director	Charlotte Benjamin		
Date	Created	2024/12/07		
	Submitted	2024/12/4		
	Approved	TBC		
	Updating Frequency	3 years		
Status	Version: 0.1			
Contributor(s)	Governance and Information Manager			
Subject	Partnership Governance			
Type	Policy			
	Vital Record		EIR	
Coverage	Middlesbrough Council			
Language	English			

Document Control

Version	Date	Revision History	Reviser
1.0	2020/02/10	First agreed policy	Ann-Marie Johnstone
1.1	2024/12/07	Refresh	Ann-Marie Johnstone

Distribution List

Version	Date	Name/Service area	Action
1.0	2020/02/10	Executive	Approval
1.1	2025/01/07	All staff via intranet	Distribution

Contact: Ann-Marie_Johnstone@middlesbrough.gov.uk

Summary

1. This policy is part of the corporate governance policy framework underpinning the Council's Council Plan and sets out how the Council will develop and manage partnerships in support of its strategic priorities for the town.
2. The following sections outline:
 - the purpose of this policy
 - definitions
 - scope
 - the legislative and regulatory framework
 - policy statement
 - roles and responsibilities
 - supporting policies, procedures and standards; and
 - monitoring and review arrangements.

Purpose

3. Partnerships are key to the Council achieving its strategic objectives. Effective partnership working is critical if we are to maximise our ability to affect change by working with whoever is best placed to deliver solutions that improve outcomes.
4. The purpose of this policy is to set out a corporate approach to partnership governance to ensure there is an effective, consistent and joined-up approach across the organisation.
5. This will deliver the following benefits:
 - ensure that proactive partnership governance is embedded within the culture of the Council, and is integral to its business planning and performance management
 - ensure that the partnership governance cycle is implemented consistently and proportionately across the Council
 - ensure that partnerships comply with the requirements of the Council's Constitution, and
 - communicate the Council's approach to partnerships to all employees and stakeholders.
6. Effective implementation of this policy will ensure that the Council understands its partnerships, how they contribute to strategic priorities, promote good governance in their operations and continuous improvement in their performance and risk management disciplines.

Definitions

Corporate governance	The systems, processes and values by which local authorities operate and by which they engage with, and are held accountable to, their communities and stakeholders.
Partnership	An arrangement in which the Council agrees to collaborate with one or more legally independent organisations to achieve shared objectives and outcomes.

Scope

7. This policy applies to all arrangements of the Council meeting the corporate definition of partnership outlined in this policy: an arrangement in which the Council agrees to collaborate with one or more legally independent organisations to achieve shared objectives and outcomes.
8. The policy applies to all elected members, employees (both permanent and temporary), contractors and consultants working for or on behalf of the Council in a partnership environment.
9. Where the Council is not lead partner, lead managers must ensure that arrangements are in line with the key principles of this policy.
10. Client and contractor relationships can be considered partnerships if they are of strategic or reputational importance to the Council, or responsible for significant public funds.
11. The following arrangements are not considered to be partnerships:
 - where the Council has complete control over decisions and funds decision-making;
 - where grants or payments are made to other organisations for services;
 - where subscriptions are made to outside bodies; or
 - procurement agreements governed under contract.

Legislative and regulatory framework

12. Key elements of the legislative and regulatory framework relevant to partnership governance are set out below.

Local Government Act 1999	General requirement to achieve best value for money. The effective governance of partnerships reduces unnecessary expenditure and increases the likelihood of delivering organisational priorities.
----------------------------------	---

Policy Statement

13. Each existing or prospective partnership will have a lead manager of appropriate seniority. The lead manager will be responsible for ensuring that partnerships are developed, governed and reviewed in line with this policy.
14. If the partnership is discretionary, then the business case for its development must be justified, and approved by the appropriate body in the Council before the Council formally enters into any partnership agreement.
15. The business case must clear how the proposed partnership will contribute to the Council’s strategic priorities in a way that cannot be achieved through an existing arrangement. It should also address how any similar partnerships may be amended or discontinued in light of the proposed new arrangement to reduce the risk of overlapping remits.
16. All formal partnership agreements and structures (incorporated partnerships or other)

will be agreed by the Monitoring Officer prior to approval.

17. All partnerships will be assessed against the governance standards set out in the Partnership Governance Framework underpinning this policy where applicable, with governance proportionate to the significance of the partnership in strategic and financial terms.
18. Partnership risks will be incorporated within the Council's risk registers where appropriate, in line with the Council's Risk and Opportunity Management Policy. It is the responsibility of the lead officer for each partner to identify where this is necessary.
19. The Council will maintain a partnership register that lists and defines all partnerships, setting out how they contribute to the Council's strategic aims and priorities. This will identify significant partnerships i.e. those that are fundamental to the delivery of strategic priorities, or meeting the Council's key decision threshold in terms of financial commitments. It will also capture key statutory partnerships.
20. An annual review of all partnerships will be undertaken, informed by an assessment of lead managers against a standard template, through which the governance and performance of the Council's partnerships will be RAG-rated and any changes recorded. This review will inform the Council's Annual Governance Statement cycle.

Roles and key responsibilities

Executive	Overall responsibility for partnership governance across the Council, including approving the Partnership Governance Policy and the creation of significant partnerships, and ensuring that partnership performance is managed, monitored and reviewed regularly.
Elected members	Members may be appointed to partnership boards and will scrutinise the performance of partnerships in line with this policy. Members must be aware of their responsibilities under the Local Code of Corporate Governance and Codes of Conduct for members and employees and ensure that the partnerships that they are involved in comply with this policy, reporting to their Group Leader and the Monitoring Officer if they consider this is not to be the case.
Audit Committee	Review the effectiveness of partnership governance and receive an annual assurance report on progress being made.
Leadership Team	Considers and approves all business cases for partnerships, ensuring that they align with the Council's strategic objectives, and reviewing quarterly performance updates and the annual partnership assessment.
Legal Services	Provides advice on partnership models and governance arrangements where appropriate and signs off all formal arrangements prior to approval.

Finance team	Provide financial input to the financial considerations that must be taken into account when establishing and managing partnerships as set out in the Financial Regulations, Section H, External arrangements 101 – 103.
Governance, Policy and information Service	Maintains the partnership register, maintain and communicates the Partnership Governance Framework, coordinates the annual partnership assessment.
Partnership Leads	Project manage the development of the partnership; act as the key point of contact between the Council and the partnership and promote the partnership within the Council; responsible for registering the partnership with Strategy, Information and Governance, providing quarterly performance updates and completing the annual partnership assessment.
Officers working in partnership	Officers working in partnerships must be aware of their responsibilities under the Local Code of Corporate Governance and Codes of Conduct for members and employees, and ensure that the partnerships that they are involved in comply with this policy, reporting to the Partnership Lead if they consider this is not to be the case.

Supporting policies, procedures and standards

21. The following policies, procedures and standards are in place that support effective partnership governance.

Information Governance Framework	Sets out a framework for effective information governance within the Council, meeting all legal obligations and underpinning the achievement of strategic objectives.
Risk and Opportunity Management Policy	Sets out how the Council will ensure that risks are effectively managed and opportunities exploited to maximise delivery of strategic objectives, fully integrated with performance management arrangements.
Performance Management Policy	Sets out how the Council will ensure that performance is effectively managed to deliver strategic priorities for the town.
Programme and Project Management Policy	Sets out how the Council will manage its portfolio of programmes and projects to ensure delivery to scope, cost, time and quality.

Monitoring and Review Arrangements

22. The Council’s expectations around partnership working are clearly set out within its corporate values and associated staff performance frameworks.

23. All managers and employees are required to comply with this Partnership Governance

Policy to ensure that the Council effectively develops and manages partnerships in support of its strategic priorities for the town.

24. An annual assurance report on the Council's partnerships arrangements will be submitted to Audit Committee. This will be supported by a targeted internal audits as appropriate, which will be listed in the Council's annual audit plan.
25. The implementation and effectiveness of this policy and its supporting procedures will be reviewed on an annual basis, using the governance assessments completed by leads of each of the partnerships.
26. This policy will be reviewed every three years, unless there is significant development that would require a more urgent review e.g. new legislation.

Appendix 1

Partnership Governance Standards

Annually, the health of partnerships should be assessed using the CIPFA 'Delivering Good Governance in Local Government' guidance as a framework to assess the following broad principles:

- Whether the partnership behaves with integrity, demonstrating a strong commitment to ethical values and the rule of law
- How the partnership ensures compliance with the principles of openness and comprehensive stakeholder engagement
- Defining outcomes in terms of sustainable economic, social and environmental benefits
- Determining the interventions necessary to optimize the achievement of the intended outcomes
- Developing the partnership's capacity, including the capability of its leadership and the individuals within it
- Managing risks and performance through robust internal control and strong public financial management
- Implementing good practices in transparency, reporting and audit to deliver effective accountability.

Within every formal partnership the following should exist, where they are applicable:

- A clear statement on aims and purpose, legal status and obligations
- Targets, objectives and outcomes and that they should be accompanied by milestones;
- Risks to the effectiveness of the partnership should be recorded and monitored
- Documented decision making and accountability rules that align with the agreed remit of the partnership and the council's constitution
- Documented meetings schedule and nominated deputies
- Agreement of the partner responsibilities and financial liabilities associated with the partnership.
- Clear and transparent financial and resourcing arrangements for finances and staffing resources
- Dispute resolution procedures and exit strategy
- An annual review of the partnership through the updating of the Partnership governance register which includes a health assessment
- Alignment with the Council's minimum standards for programme and projects where the Council is the lead partner
- An assessment completed on an annual basis of the health of the partnership.

This page is intentionally left blank

MIDDLESBROUGH COUNCIL	
------------------------------	--

Report of:	Director of Legal and Governance Services
Submitted to:	Individual Executive Member Decision-Making: The Mayor
Date: TBD	17 December 2024
Title:	Surveillance Policy 2024/5
Report for:	Decision
Status:	Public
Council Plan priority:	Delivering Best Value
Key decision:	No
Why:	Decision does not reach the threshold to be a key decision
Subject to call in?:	Yes
Why:	Not urgent

Proposed decision(s)	
That the Mayor:	
<ul style="list-style-type: none"> • AGREES the annual review of the Surveillance Policy. 	

Executive summary	
<p>This report seeks approval of an updated Surveillance Policy. In accordance with the Statutory Codes of Practice applying to the Regulation of Investigatory Powers Act 2000 (RIPA) The Authority is required to review its use and set out the Policy at least annually.</p>	

Purpose

1. This report presents seeks approval of the proposed corporate Surveillance Policy 2024/25.
2. Guidance underpinning the Regulation of Investigatory Powers Act (RIPA) 2000 states that elected members should review the Council's use of RIPA powers and set the RIPA policy at least once per annum.
3. Use of RIPA powers are considered annually by Audit Committee as part of the annual report of the Senior Information Risk Owner. Statistical information on use of the powers will be reported to a future meeting of the relevant Scrutiny Panel.

Recommendations

4. That the Mayor:

AGREES the annual review of the Surveillance Policy.

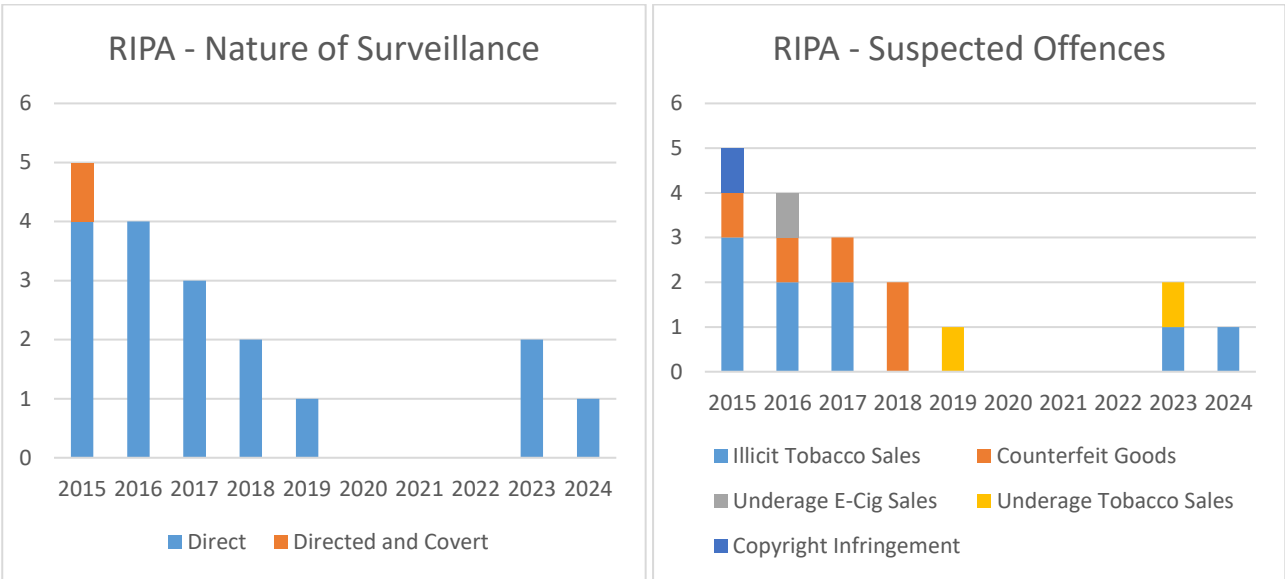
Rationale for the recommended decision(s)

5. The proposed policy will ensure that surveillance activity undertaken by the Council complies with its strategic priorities and statutory obligations, is lawful and that due regard is given to human rights and to data protection rights.

Background and relevant information

Use of RIPA

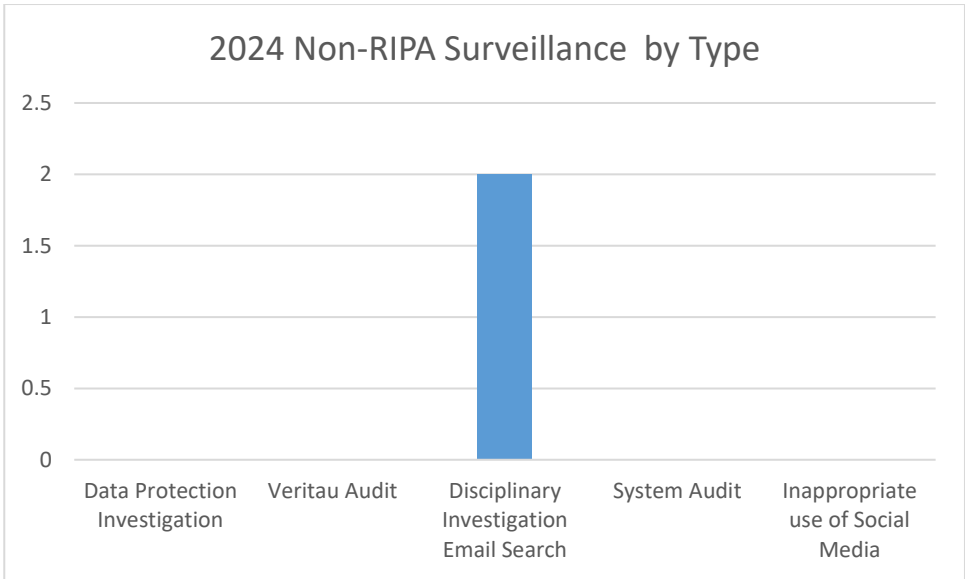
6. RIPA is the law governing the use of surveillance techniques by public authorities, including local authorities. RIPA requires that when public authorities need to use covert techniques to obtain private information about someone, they only do so if surveillance is necessary, proportionate, and compatible with human rights. Typically, this relates to suspected criminal activity that is likely to result in a custodial sentence of six months or more.
7. In such instances, covert surveillance can be undertaken, subject to magistrate approval, if it is not possible to gather sufficient evidence to secure a prosecution without this.
8. The charts below set out the past ten years of RIPA activity undertaken by the Council, the nature of the surveillance and the reasons why it was undertaken. To note, the Council always looks to methods to gather information that do not require covert surveillance to be undertaken, in order to minimise use of this power, therefore activity remains low.



9. Since this policy was last reviewed, one RIPA application was submitted in 2024.

Non-RIPA surveillance

10. The Council also has in place a process, set out within the Surveillance policy, which governs the application of requests for surveillance on non-RIPA grounds. The data for 2024 relates to staffing matters, these are centrally logged and approved by HR to again ensure the use of this power is minimised and there is a legitimate basis for use is identified prior to approval. The table below sets out the reasons this power used to investigate the following potential issues:



Monitoring and review

- 11. This Policy is updated annually and was last approved by the Executive Member for Finance and Governance in December 2023.
- 12. As was agreed with the IPCO following their last inspection in late 2020 we continue to maintain an overarching Surveillance Policy (Appendix 1), which covers CCTV, RIPA, non-RIPA covert surveillance and the surveillance of employees.
- 13. The Council’s policy aligns with guidance published by the Information Commissioners Office on monitoring workers.
- 14. The Surveillance policy review this year has had minor changes to reflect staffing, no other change has been necessary.

Other potential alternative(s) and why these have not been recommended

- 15. The Council could choose to restrict this policy to RIPA activity only and develop and implement separate policies relating to non-RIPA surveillance, employee surveillance and other issues not currently covered by policy. However, this is not recommended, as a single policy provides for a coherent and systematic approach and is in line with the Council’s commitment to openness and transparency.

Impact(s) of the recommended decision(s)

Topic	Impact
Financial (including procurement and Social Value)	It is anticipated that all activities require by the policy are achievable within existing and planned budgets.
Legal	The report and its associated action plan, demonstrates how the Council does and will continue to meet its various legal duties when undertaking surveillance.
Risk	Implementation of the proposed Surveillance Policy mitigates a number of risks within the Council’s strategic and information risk registers, having a positive overall impact on the strategic risk that the Council could fail to comply with the law.
Human Rights, Public Sector Equality Duty and Community Cohesion	The proposed policy has been subject to Level 1 (screening) equality impact assessment (at Appendix 2). This assessment identified that no negative differential impacts on diverse groups and communities within Middlesbrough is anticipated from the implementation of the policy.
Climate Change / Environmental	There are no climate or environmental impacts associated with the proposed policy.
Children and Young People Cared for by the Authority and Care Leavers	There are no direct implications arising from this Policy on this group as identified in the equality impact assessment (Appendix 2).

Data Protection	This policy aims to balance the business interests of the Council as an employer and workers' rights and freedoms under data protection law. It is imperative that the Council has an up-to-date policy which advises staff on proper use of these powers to ensure any action is lawful, necessary and proportionate.
-----------------	--

Actions to be taken to implement the recommended decision(s)

Action	Responsible Officer	Deadline
Publication of surveillance policy on the MBC Website and Intranet pages	L Hamer	5 January 2025
Senior Information Risk Owner (SIRO) annual report to Corporate Affairs and Audit Committee	Ann-Marie Johnstone	April 2025

Appendices

1	Surveillance Policy 2024/2025
2	Surveillance Policy 2024/25 – Impact Assessment Level 1: Initial screening Assessment

Background papers

Body	Report title	Date
Executive Member for Finance and Governance	RIPA Policy	28/02/2020
Corporate Affairs and Audit Committee	Annual Report of the Senior Information Risk Owner (SIRO)	29/04/2021
Executive Member for Environment, Finance and Governance	Surveillance Policy	10/08/2022
Corporate Affairs and Audit Committee	Annual Report of the Senior Information Risk Owner (SIRO)	31/03/2022
Corporate Affairs and Audit Committee	Annual Report of the Senior Information Risk Owner (SIRO)	April 2023
Executive Member for Finance and Governance	Surveillance Policy	20 December 2023

Contact: Ann-Marie Johnstone, Head of Governance, Policy and Information
Email: ann-marie_johnstone@middlesbrough.gov.uk

This page is intentionally left blank



Surveillance Policy

Creator	Author(s)	Ann-Marie Johnstone		
	Approved by	Executive Member		
	Department	Legal and Governance Services		
	Service area	Policy, Governance and Information		
	Head of Service	Ann-Marie Johnstone		
	Director	Charlotte Benjamin		
Date	Created	2022/09/15		
	Submitted	2022/10/05		
	Approved	2022/12/14		
	Updating Frequency	Annually, unless review triggers met in interim		
Status	Version: 9.0			
Contributor(s)	Governance and Information Manager; Data Protection Officer, HR Manager, Operational Community Safety Manager			
Subject	Overt and covert surveillance			
Type	Policy			
	Vital Record		EIR	
Coverage	Middlesbrough Council			
Language	English			

Document Control

Version	Date	Revision History	Reviser
6.0	2021/07	Review – move to Surveillance Policy	P Stephens
7.0	2022/12	Review	AM Johnstone
8.0	2023/11	Review	L Hamer
9.0	2024/11	Review	AM Johnstone

Distribution List

Version	Date	Name/Service area	Action
7.0	2022/12	All stakeholders	Note
8.0	2023/11	All stakeholders	Note
9.0	2024/11	All stakeholders	Note

Contact: data@middlesbrough.gov.uk

Summary

1. This policy provides a framework for the undertaking of surveillance by the Council of the public and of its employees, where appropriate, ensuring that any surveillance undertaken is lawful and that due regard is given to human rights and to data protection rights.
2. The following sections outline:
 - the purpose of this policy;
 - definitions;
 - scope;
 - the legislative and regulatory framework;
 - roles and responsibilities;
 - policy detail;
 - supporting policies, procedures and standards; and
 - monitoring and review arrangements.

Purpose

3. This policy provides a framework for undertaking surveillance activities in compliance with all applicable laws by:
 - creating and maintaining organisational awareness of the Right to Privacy (Article 8, Human Rights Act 1998) as an integral part of operations;
 - ensuring that all employees are aware of and fully comply with the relevant legislation as described in this policy and fully understand their own responsibilities when planning and undertaking surveillance activities;
 - where necessary, ensuring that all employees obtain the appropriate authorisations when undertaking surveillance activities; and
 - ensuring that sensitive and confidential surveillance information is stored, archived and disposed of in an appropriate manner.

Definitions

4. Appendix 1 defines the key terms used in this policy. Where appropriate, the definitions used by the Council are aligned with those in legislation or supporting codes of practice.

Scope

5. The policy applies to all overt and covert surveillance undertaken by or on behalf of the Council. This includes, but is not limited to the following:
 - the taking of photographs of someone in a public place;
 - the recording by video cameras of someone in a public place;
 - the use of listening devices or photographic equipment to obtain information in respect of activities in a residential premises or private vehicle;
 - the acquisition of communications data from third party service providers;
 - the viewing of someone's social media activity;
 - the taking of photographs of employees in the workplace;

- the recording by video cameras of employees in the workplace;
 - the viewing of an employee's social media activity; and
 - the acquisition of employees' communication data or other tracking data during the course of work.
6. At this time the Council does not use drones for surveillance or enforcement purposes.
 7. The policy applies to all Council employees and any other party undertaking surveillance on behalf of the Council by contract. Non-compliance with this policy may result in disciplinary action or other sanction, with the individual(s) responsible for non-compliance held personally accountable for any breaches of Article 8 of the Human Rights Act 1998.
 8. This policy is approved and its application scrutinised by elected members but members will have no direct involvement in surveillance operations or in making decisions on specific authorisations.
 9. The policy does not apply to householders or businesses who have obtained grants from the Council for the purpose of installing domestic or commercial CCTV. Equipment paid for and installed under these grants is not the property of the Council and the Council has no legal responsibilities for such equipment or the information obtained by its use.

Legislative and regulatory framework

10. The Council must comply with all relevant applicable legislation pertaining to surveillance, as outlined below.

Human Rights Act 1998

11. The Human Rights Act 1998 (HRA) gave effect in UK law to the rights set out in the European Convention on Human Rights (EHCR).
12. The HRA requires that all action which may potentially impact on an individual's human rights is proportionate, necessary, non-discriminatory and lawful. The HRA lists sixteen basic human rights, which are either absolute, limited or qualified. All activity undertaken by the Council must comply with the HRA, including surveillance.
13. Article 8 of the EHCR – the qualified right to respect for private and family life, home and correspondence – is most likely to be engaged when local authorities seek to obtain private information about a person by means of surveillance. Covert surveillance, in particular via RIPA, are likely to engage the limited right to a fair and public hearing (Article 6).

Regulation of Investigatory Powers Act 2000

14. Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) does not grant powers to undertake surveillance but does provide a statutory framework under which appropriate covert surveillance activity undertaken by local authorities (specifically directed surveillance and the use of CHIS) can be authorised, conducted

and supervised compatibly with Article 8 of the ECHR and the Data Protection Act 2018.

15. RIPA aims to balance the rights and freedoms of individuals with the need for law enforcement and security agencies to have powers to perform their roles effectively.
16. The grounds on which local authorities can rely on to authorise directed surveillance are narrower than those available to security services or the police. A local authority can only authorise directed surveillance of a member of the public if the designated person believes that such surveillance is necessary and proportionate for the purpose of preventing or detecting a crime which the local authority has legal powers to prosecute. In most cases the threshold is an offence for which there is a minimum prison sentence of six months, and the surveillance must also be authorised by a magistrate.
17. The acquisition of a RIPA authorisation will equip the Council with the legal protection (the RIPA 'Shield') against accusations of a breach of Article 8. Failure to comply with RIPA does not necessarily mean that surveillance would be unlawful, however it does mean that evidence obtained from surveillance could be inadmissible in court proceedings and so jeopardise a successful outcome. Unauthorised action could also be open to challenge as a breach of the HRA and a successful claim for damages could be made against the Council.
18. Appendices 3 to 6 set out the forms that must be completed when applying for authority to conduct directed surveillance using RIPA, renewing authorisation and cancelling directed surveillance. Appendices 7 to 10 set out the same process for use of Covert Human Intelligence Sources using the RIPA legal framework.
19. A number of Codes of Practice have been issued under Part II of RIPA, as listed below. This policy and its supporting procedures fully comply with these codes.

[Interception of communications: code of practice 2016](#)

[Equipment interference: code of practice](#)

[Codes of practice for the acquisition, disclosure and retention of communications data](#)

[Covert surveillance and covert human intelligence sources codes of practice](#)

[Code of practice for investigation of protected electronic information](#)

[Employment practices and data protection: monitoring workers | ICO](#)

Data Protection Act 2018

20. Middlesbrough Council is a 'competent authority' for the purposes of Part 3 of the Data Protection Act 2018 (DPA) where it has authority or powers to investigate and prosecute criminal offences.
21. In this role the Council will comply with the law enforcement principles, which are reflected within this policy as appropriate. Processing of personal data for any of the law enforcement purposes must be:
 - lawful and fair;
 - collected and only processed for a specified, explicit and legitimate purpose;
 - adequate, relevant and not excessive;

- accurate and, where necessary, kept up to date, and that personal data that is inaccurate is erased or rectified without delay;
- kept for no longer than is necessary and storage periodically reviewed; and
- processed in a manner that ensures appropriate security.

22. All other personal data that is not processed for law enforcement purposes falls under the UK General Data Protection Regulation 2016 (UK GDPR) and other applicable Parts of the DPA including appropriate exemptions (referred to as ‘the data protection legislation’). In this general processing role, as a data controller, the Council will comply with the GDPR principles, which are reflected in this policy as appropriate.

23. Personal data will be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary; and
- processed in a manner that ensures appropriate security of the personal data.

24. As a data controller, the Council will be responsible for, and be able to demonstrate compliance with these principles.

Protection of Freedoms Act 2012

25. The Protection of Freedoms Act 2012 (POFA) provides for a wide range of measures to protect and promote the freedoms of individuals. Part 2 of the POFA required a new Code of Practice on surveillance technologies and the appointment of a Surveillance Camera Commissioner to oversee and review the operation of the Code.

26. A Surveillance Camera Code of Practice was published in 2013 and provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities and sets out 12 guiding principles that should be adopted by systems operators:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

27. POFA also amends s28 of RIPA and brought in the requirement for a magistrate to approve a RIPA authorisation when the crime threshold is met. The threshold is a criminal offence which attract a minimum custodial sentence of six months or more. There are some limited exceptions to the six month rule, specifically:

- the sale of alcohol to children (S.146 of the Licensing Act 2003);
- allowing the sale of alcohol to children (S.147 of the Licensing Act 2003);
- persistently selling alcohol to children (S.147A of the Licensing Act 2003); and
- the sale of tobacco to persons under 18 years of age (S.7 Children and Young Persons Act 1933).

Investigatory Powers Act 2016

28. The Investigatory Powers Act 2016 (IPA) commenced on 11 June 2019 and is now the main legislation governing local authorities' access to communications data in order to carry out their statutory functions as a 'competent authority' under the DPA, replacing the framework set out in RIPA.

29. The Communications Data Code of Practice sets out the process for acquiring communications data in line with the Act.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

30. These regulations implemented Article 5 of the EU Telecoms Privacy Directive and gave businesses the right to intercept communications on their own networks, which occur as part of lawful business practice, and for the certain purposes.
31. Interception is lawful for the purposes of monitoring or recording, if doing so:
- allows the business to comply with other regulations;
 - establishes the existence of facts;
 - acts as a means of verification that the person being monitored is performing his or her work to standards;
 - is in the interests of UK security;
 - may prevent or detect criminal activity;
 - ensures the communication system operates effectively; and
 - allows the business to detect unauthorised use of the system.

Employment Practices Code

32. The Information Commissioner's Office's Employment Practices Code provides a framework under which surveillance of the activity of employees can be authorised and conducted compatibly with Article 8 of the ECHR and the DPA. It covers amongst other matters, how employees can be monitored in the workplace and their right to work in a comfortable environment. Monitoring of employees should only take place where there is a real risk to the business and in line with the DPA, employees should be told about monitoring practices and under what circumstances their communications might be intercepted. A form that must be completed for the authorisations is in place and available on the Council's intranet page. Authorisations must be approved by the HR Manager.

Key roles and Responsibilities

33. Effective and lawful surveillance is the collective responsibility of all those individuals named within the scope of this policy. Appropriate training will be provided to all those officers within the scope of this policy.
34. As with all Council policies, Directors and Heads of Service have a general responsibility to ensure compliance with this policy within their operations. This includes taking reasonable steps to protect the health and safety and where appropriate third parties involved in surveillance, including the carrying out of risk assessments.
35. The specific roles within surveillance activities are described below. Where appropriate, the current role holders and their deputies are listed at Appendix 2.

Senior Responsible Officer (SRO)

36. The SRO has overall responsibility for overt and covert surveillance, including:
- creation, communication and review of this policy;
 - appointing the CCTV Single Point of Contact;
 - acting as the Senior Responsible Officer for CCTV
 - appointing the Coordinating Officer (Auditor) for covert surveillance;
 - ensuring the availability of appropriate authorisers for covert surveillance;

- raising corporate awareness of the policy and proper surveillance practices;
- assessing corporate compliance with this policy;
- providing professional guidance on all matters relating to surveillance;
- engagement with the Surveillance Camera Commissioner and the IPCO; and
- overseeing the implementation of any post-inspection action plans recommended or approved by the IPCO.

Overt surveillance

37. The following key roles are in place in relation to **overt** surveillance via cameras and other equipment:

CCTV Single Point of Contact (SPOC)

38. Appointed by the SRO, and supporting the Data Protection Officer, the SPOC will ensure the Council operates all surveillance camera equipment in compliance with the Surveillance Camera Code and key legislation, thereby building transparency, trust and confidence.
39. Specifically, the SPOC will:
- establish and maintain a CCTV code of practice setting out the regulatory framework that each Council scheme must comply with, the internal assessment programme that each scheme must undertake and the processes required to establish a new surveillance camera scheme or upgrade an existing scheme;
 - maintain a central register of all public space surveillance camera equipment operated by the Council, including the location of each piece of equipment, its asset reference and the manager responsible;
 - act as the main point of contact for surveillance camera systems, and introduce consistent procedures that can be applied across all systems in operation, including standardised signage, alongside appropriate training for those operating surveillance cameras; and
 - provide regular guidance and updates to scheme managers to ensure that all surveillance cameras schemes continue to operate in full compliance with the regulatory framework governing its use and undertake an annual audit of all schemes, documented in an annual report to the SRO.

Scheme Managers

40. A scheme manager will be in place for each individual scheme operated by or on behalf of the Council. Scheme managers will maintain the following documentation in a Code Assessment Pack, which will demonstrate compliance with the local code and allow the SPOC to undertake their role.
- list of all documents maintained by the scheme manager;
 - scheme asset list – a complete record of all cameras, signage, monitors and recording equipment, with location, functionality and purpose and associated contractual arrangements for management and / or maintenance;
 - record of data protection impact assessments (DPIAs) for each camera (or if agreed, groups of cameras) on the asset list and cyber security checks undertaken;

- scheme access list – including who is authorised to access the scheme and the level of access granted;
- training records of all those accessing the scheme and associated confidentiality arrangements;
- records of the self-assessment and annual review, including who undertook this and the changes made as a result; and
- declaration of compliance – completed annually or when the scheme manager changes.

Responsible Officers

41. All CCTV sites also should have an appointed Responsible Officer (RO) – this may or may not be the scheme manager. ROs are responsible for the day-to-day management of the CCTV system and providing relevant information to the scheme manager.

Surveillance Camera Operators

42. All surveillance camera operators or those otherwise viewing images will undertake training relevant to operating public space surveillance, information security and personal data. They will be required to sign appropriate confidentiality agreements.

Covert surveillance

43. The following key roles are in place in relation to **covert** surveillance:

Coordinating Officer (Auditor)

44. The Coordinating Officer (Auditor) will:
- provide up-to-date guidance and training on covert surveillance within the Council;
 - maintain a central record of authorisations including a Unique Reference Number (URN);
 - audit each covert surveillance application, authorisation, review, renewal and cancellation for compliance with this policy and the law, ensuring there is a uniformity of practice; and
 - advise the SRO as appropriate in the light of the above.

Authorising Officers

45. Authorising Officers will assess, authorise, renew and cancel all public-facing covert surveillance (RIPA or non-RIPA) on behalf of all Directorates. Authorising Officers will be at Head of Service level or above, trained to an appropriate standard, and cannot authorise surveillance requested by any service or team under their management.
46. The SRO will ensure there is always a minimum of three trained authorising officers within the Council. The SRO will authorise surveillance in exceptional circumstances.
47. If confidential information or matters subject to legal privilege are likely to be acquired through directed surveillance or by a Covert Human Intelligence Source (CHIS), or

the CHIS is a juvenile aged between 16-18 years or a vulnerable adult, the surveillance may only be authorised by the Head of Paid Service.

48. Covert surveillance of employees will only be permitted during an investigation of an allegation of a serious disciplinary offence and will be authorised by the HR Manager and an authorising officer. A form is in place to ensure compliance with this policy for non-RIPA directed surveillance.

IPA Single Point of Contact (SPoC) (Communications data)

49. The National Anti-Fraud Network (NAFN) acts as the SPoC for the Council for the acquisition of external communications data, liaising with the Office for Communications Data Authorisations on the Council's behalf.

IPA Designated Person (Communications data)

50. The Designated Person (Communications data) approves telecommunications applications that have been checked by the IPA SPoC.

Applicants (Case Officers)

51. Only officers that can reasonably be expected to undertake covert surveillance as part of their job description will plan and apply for the authorisation of such surveillance for RIPA based surveillance. Line Managers may apply to conduct non-RIPA based surveillance of an employee by accessing communications, tracking or other data but must have the approval of the HR Manager, unless there is a reason why they should not be made aware of the surveillance. In that case the reason must be set out in the application and the approval of the SRO sought. In some restricted circumstances, there may be a need to consider covert surveillance of the public in circumstances where the RIPA threshold would not be met but the Council may have a legitimate need to gather information in order to assess fraud, defend a legal case or investigate in line with its statutory duties. Where this is the case, an authorisation process must be followed where the need to gather evidence would exceed the threshold for surveillance.

Policy detail

52. The Council will use overt and covert surveillance within its operations where it is appropriate to do so.

Overt surveillance

53. Most of the surveillance carried out by the Council will be done overtly e.g. general observations made by officers in line with their job roles and legal powers.
54. Overt surveillance using relevant equipment will be undertaken in line with the national Surveillance Camera Code of Practice. The Council will maintain a local code of practice that fully complies with the national code and keep this up to date.
55. The SRO will appoint a SPoC for CCTV and notify the Surveillance Camera Commissioner accordingly.

56. The SPoC will oversee all CCTV schemes operated by or on behalf of the Council and ensure their compliance with the national and local codes.
57. Scheme managers and responsible officers will be identified for all schemes and they will maintain Code Assessment Packs, demonstrating compliance with the Council's local code of practice.
58. Scheme managers will ensure that DPIAs are undertaken before any surveillance system is installed, whenever new technology or functionality is being added onto or removed from an existing system, or whenever there are plans to process more sensitive data or capture images from a different location.
59. Scheme managers will ensure that responsible officers and surveillance camera operators working within their schemes are trained to the standard required by the Council's Code of Practice and have signed appropriate confidentiality agreements.
60. The SPoC will produce an annual report based on a review of annual self-assessments from scheme managers. The annual report will cover all schemes and equipment operated by the Council, covering:
 - operating arrangements, including contracts;
 - performance of schemes;
 - compliments and complaints received;
 - outcome of any inspections or audits in the year;
 - assurance the scheme continues to operate in compliance with legislation and relevant codes of practice; and
 - whether the scheme and / or individual cameras are still required.
61. From time to time, the Council may offer grants to residents for the installation of domestic CCTV systems. Equipment paid for and installed under these grants is not the property of the Council and the Council has no legal responsibilities for such equipment.
62. Outside of contractual arrangements, the Council will not direct any third party to undertake surveillance on its behalf. Any footage provided to the Council as potential evidence of criminality will only be processed where the Council has a lawful basis to do so and where the footage has been captured in line with data protection legislation.

Overt use of recording – virtual meetings

63. From time to time, officers within the Council may identify a legitimate need to record an online interaction using the Council's meeting software tools, or those of any Council supplier, excluding the streaming and recording of formal member committee meetings which are open to the public. Any officer wishing to do this must first assure themselves that recording the interaction is necessary and proportionate to the purpose identified having sought advice from the Data Protection Officer and prior approval from the Senior Information Risk Owner. There is a process in place to govern when formal committee meetings of the Council will be recorded.

Covert surveillance

64. The Council will use covert surveillance to acquire information to support investigations where it is lawful and appropriate to do so.
65. Covert surveillance will only be used where it is not considered possible to obtain the necessary information to progress investigations by overt means e.g. interview. In addition, the method of surveillance must be proportionate and the least harmful means of gathering the information.
66. Covert surveillance does not require authorisation when it is in immediate response to events and it is not reasonably practicable for authorisation to be sought e.g. CCTV tracking of a crime in progress to assist police detection of offenders. When covert surveillance has been used in such circumstances it will be noted in the incident report(s) of the employee(s) that have undertaken the surveillance.
67. In the majority of circumstances, however, covert surveillance will be directed, planned, and authorised, through either (i) the framework provided by the Regulation of Investigatory Powers Act 2000, or (ii) internal authorisation processes that follows the spirit and principles of RIPA to ensure that such covert surveillance is necessary, proportionate, non-discriminatory, uses suitable equipment, and is lawful. This is set out in the supporting forms at appendices 3 to 6.
68. The Council will carry out covert surveillance to progress investigations outside of the RIPA framework, where (i) while significant, the matters under investigation may not typically result in criminal proceedings, or (ii) the potential criminal offence(s) under investigation are likely to attract a penalty below the RIPA threshold. Examples of such instances include but are not limited to:
- suspected benefit fraud;
 - children at risk as court orders are not being respected;
 - serious cases of anti-social behaviour; or
 - contractors failing to carry out contracted works.
69. Both RIPA and non-RIPA surveillance will use a systematic process of:
- application;
 - authorisation;
 - conduct of authorisation;
 - review;
 - renewal (where necessary); and
 - cancellation.
70. The following standard forms for RIPA applications will be used and provided via the Coordinating Officer (Auditor). Forms for internal authorisation of non-RIPA covert surveillance are also in place.
- Application for use of directed surveillance
 - Review of use of directed surveillance
 - Renewal form for directed surveillance
 - Cancellation of use of directed surveillance form
 - Application for the use of covert human intelligence sources (CHIS)
 - Reviewing the use of covert human intelligence sources (CHIS)

- Renewal of authorisation to use covert human intelligence sources (CHIS)
- Cancellation of covert human intelligence sources (CHIS)

Application

71. Only officers that can reasonably be expected to undertake covert surveillance as part of their job description will plan and apply for the authorisation of such surveillance.
72. At the start of an investigation, the applicant will consider whether the alleged activity proposed for surveillance is a potential criminal offence that meets the RIPA threshold, as defined within this policy.
73. If this threshold is met, the applicant will complete the mandatory RIPA application form (directed surveillance and / or CHIS). If the threshold is not met, then the applicant will complete and submit the Council's non-RIPA application form.
74. Both forms provide for consideration of necessity and proportionality and the likelihood of collateral intrusion and gathering confidential information, and how this can be mitigated. In completing the form(s), the applicant will have regard to the relevant code(s) of practice, the Council's covert surveillance procedure and associated guidance, and be advised by the SRO, Coordinating Officer (Auditor) and / or Legal Services where required.
75. The applicant considers the surveillance to be justified following completion of the forms, then a URN should be obtained from the Coordinating Officer (Auditor) and the form submitted to an appropriate authorising officer as defined by this policy for authorisation.

Authorisation

76. Authorisation is an appropriate safeguard against the abuse of power by public authorities. The appropriate authorising officer will assess the request for authorisation applying the same tests and the applicant, ensuring that a defensible case can be made for the conduct to be authorised.
77. In completing the form(s), the authorising officer will have regard to the relevant code(s) of practice, the Council's covert surveillance procedure and associated guidance, and be advised by the SRO, Coordinating Officer (Auditor) and / or Legal Services where required.
78. Having taken these issues into account, the authorising officer will either approve, part-approve or reject the application, updating the form(s) in writing. The authorising officer cannot add activity that they may wish to see on to the application.
79. The authorising officer will notify the applicant and the Coordinating Officer (Auditor) of the decision reached.
80. Before an authorisation can take effect it must be approved by a Justice of the Peace (a District Judge or Magistrate) in the case of RIPA applications, or the SRO, in the

case of non-RIPA applications. The Coordinating Officer will liaise with the applicant, Legal Services and the SRO as required to secure the appropriate approvals.

81. In urgent cases (i.e. a likelihood of endangering life or jeopardising an investigation if authorisation is not immediate), verbal authorisation may be sought and authorisation recorded in writing. An urgent verbal authorisation may last for 72 hours. However, if the surveillance continues and there is opportunity before the expiration of 72 hours, authorisation in writing should be applied for and authorised if appropriate.
82. Written authorisations for directed surveillance last for a fixed duration of three months and CHIS for 12 months (or one month in the case of a juvenile CHIS) from the date of the magistrate's approval. The Council will apply the same duration to non-RIPA authorisations.
83. Written authorisations for non-RIPA applications will be considered by the SIRO as authorising officer.

Conduct of authorisation

84. It will be the responsibility of the applicant and those conducting the authorised surveillance to ensure that it is done appropriately, ensuring:
 - surveillance is carried out in accordance with the authorisation;
 - collateral intrusion is monitored and minimised as far as possible;
 - intrusive surveillance is not carried out under any circumstances; and
 - information obtained is recorded and managed appropriately.
85. Any CHIS (RIPA only) used must be aware that:
 - only the tasks authorised must be carried out;
 - collateral intrusion is minimised as far as possible;
 - intrusive surveillance is not carried out under any circumstances
 - entrapment is not permitted; and
 - they must report only to the applicant.
86. If the authorised activity unexpectedly interferes with the privacy of individuals not covered by the authorisation, if the conduct or health safety of a CHIS becomes a concern, or any other unforeseen event occurs, the applicant must report this to the authorising officer, who will consider whether the authorisation should be amended or cancelled.

Review

87. All authorisations for covert surveillance or use of a CHIS (RIPA only) will be reviewed by the applicant using the appropriate form every 28 days, or sooner if the risk of collateral intrusion or of obtaining private information is high or the circumstances of the investigation require it.
88. The applicant will send the completed form to the relevant authorising officer and the coordinating officer.

Renewal

89. If towards the end of the authorisation period there is a case for continuing the covert surveillance, the applicant will complete the appropriate form and send to the relevant authorising officer for consideration.
90. If the authorising officer agrees that the grounds for authorisation remain in place then the form will be sent to the coordinating officer to arrange consideration by a JP for RIPA applications.
91. If the authorisation lapses during this period then no further surveillance can be undertaken until the JP has approved the renewal for RIPA applications.
92. Subject to approval, directed surveillance can be extended for a further three months and an adult CHIS for a further 12 months, starting on the date of the day the previous authorisation ended.
93. For non-RIPA applications, renewal applications for surveillance will be considered by the SIRO as authorising officer.

Cancellation

94. There is a presumption that covert surveillance or CHIS authorisations (RIPA only) will be cancelled at the earliest opportunity using the appropriate form.
95. Authorisations **must** be cancelled if the authorisation period has not ended and:
 - conditions for authorising the surveillance are no longer satisfied;
 - sufficient information has been gathered to progress litigation; or
 - it is clear that no evidence of the suspected activity will be detected.
96. Authorisations must also be cancelled when the authorisation period has expired and a renewal has not been requested and authorised.
97. The applicant will send the completed form to the relevant authorising officer and the coordinating officer.

Errors

98. All errors in documentation must be reported immediately by the authorising officer to the SRO for consideration and appropriate action.

Covert Human Intelligence Sources (CHIS)

99. The Council will use CHIS to acquire information covertly where it is lawful and appropriate to do so. The crime threshold does not apply to the authorisation of a CHIS.
100. Individuals contacting the Council to provide unsolicited information on a one-off basis will not be considered CHIS.

101. Similarly, those individuals undertaking test purchases on behalf of the Council will be trained to ensure that they do not form a relationship other than that of customer / retailer, and these individuals will also not be considered CHIS.
102. If however that individual proceeds to pass on more information and this includes forming a relationship with other parties to facilitate this, then a CHIS application will be made. Officers must be conscious of the prospect of individuals drifting into the status of CHIS in their desire to assist the Council and take appropriate actions to advise and safeguard such individuals where necessary.
103. The Council will not authorise the use of a juvenile as a CHIS against their parents or carers. The Council will not authorise the use of a juvenile or a vulnerable adult as a CHIS without undertaking a specific risk assessment. Authorisation of such an individual as a CHIS can only be approved by the Head of Paid Service. Forms set out at appendices 7 to 10 of this policy set out the detail required for the approval, review and cancellation of CHIS surveillance requests.

Other third parties

104. Where the Council has instructed another agency to act on its behalf under RIPA, this policy and its associated procedures and forms will apply. Applicants will ensure that third parties are aware of exactly what they are authorised to do.
105. Two or more public authorities can undertake a joint directed surveillance investigation or use of a CHIS. In such circumstances it must be clear which authority will lead the investigation and so authorise the surveillance.
106. Requests from third parties to use the Council's equipment, facilities and / or buildings under RIPA authorisations must be made in writing (including a copy of the authorisation, redacted where appropriate) to the SRO, or in the case of CCTV, the SPoC.

Telecommunications data

107. The Council can apply for individual's telecommunications data in support of investigations where appropriate. Applications can be made for entity and event data. The crime threshold applies only to event data.
108. Applicants for telecommunications data must complete the appropriate forms, which will be provided by the Designated Person. Applications will be routed through the IPA SPOC, NAFN, which will check for legal compliance and submit applications to the OCDA once approved by the Council's Designated Person.
109. Any application returned by the OCDA for re-work must be completed within 14 days or a new request must be submitted. Any application rejected by the OCDA can be appealed within seven days, via the Designated Person.

Online surveillance

110. Websites and social media are another source of intelligence for investigations.

111. In general terms, overt monitoring of online material, where the subject has been informed that this is taking place, or the preliminary reconnaissance by Council officers of websites or the social media sites of individuals to ascertain whether they may be of interest, and that do not involve any personal interaction, will be unlikely to require authorisation as they are unlikely to interfere with an individual's reasonably held expectation of privacy.
112. In all other circumstances (e.g. repeated visits to sites to gather information, or establishing a relationship with a viewing to purchasing items either directly or through a CHIS) will likely require authorisation as set out in this policy.
113. Officers will not use covert profiles online. If an investigation requires covert profiles then this should be undertaken by the police or specialists in regional or national trading standards teams.
114. The Council will set out in its privacy notices where it may gather information from online sources as part of its investigations, including the lawful condition relied upon.
115. In undertaking online surveillance, officers will have regard to the relevant code(s) of practice, the Council's covert surveillance procedure and associated guidance, and be advised by the SRO, Coordinating Officer (Auditor) and / or Legal Services where required.

Surveillance of employees

116. All employees are entitled to a comfortable working environment that provides an appropriate degree of privacy, consistent with data protection legislation. However, the monitoring of employees is necessary under certain circumstances in order to safeguard employees, customers and the Council as an employer.
117. The Council will be clear with employees and Trade Unions when, under what circumstances and to what extent, monitoring and surveillance – both overt and covert – will be used in the workplace.
118. All monitoring and surveillance of employees will be proportionate and in line with the guidance issued by the Information Commissioner to ensure employees' personal data is respected and properly protected under the data protection legislation. In order to lawfully monitor employees, the Council must identify its lawful basis for doing so and identify a special category processing condition if sensitive data is likely to be captured. The Information Commissioner's Office provides an interactive tool to support applicants to understand the lawful basis for planned monitoring.¹
119. Employees will be routinely captured on CCTV during the course of their work. Some employees have been given access to devices which offer the option of using biometric data to secure the device. Where an employee has opted into that device, any data gathered will be held on the device and only used for that purpose.
120. The Council will also collate and retain records of employee communications data, including but not limited to, door entry, vehicle, safety tracking devices, ICT device,

¹ <https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/>

network, system and internet access and usage, instant messaging, telephone calls and printing logs, in line with its retention schedule.

121. Employees will be clearly advised as to what represents appropriate and fair private usage of the systems set out above. In some cases the Council will not permit the private use of such systems at all.
122. The content of phone calls and online meetings involving employees will only be recorded where there is prior notification to the caller e.g. into the Council's contact centre.
123. The Council will use GPS trackers on all of its fleet vehicles and also provide them to certain individuals in line with their job roles or working arrangements e.g. neighbourhood wardens, lone workers. Alertcom users.
124. The Council will not track any individual through their work-provided mobile phone or other devices unless there is considered to be a threat to the individual's or other relevant person's health and safety or tracking is incidental e.g. attempting to locate a device that has been reported as lost, missing or stolen.
125. The Council will undertake drug and alcohol testing for employees where there is reasonable cause and post-incident (e.g. after a road traffic accident).
126. CCTV footage of employees may be used to investigate a crime or incident of anti-social behaviour, or to investigate a security or health and safety incident.
127. Employee communications will be legitimately accessed and utilised in the investigation of management investigations, complaints and in response to statutory information requests from members of the public.
128. Routine monitoring of systems access will be undertaken to ensure that employee access to customer personal data is lawful and appropriate.
129. Outside of the above, access to internal CCTV footage and employee communications data and the covert surveillance of employees through these means will only be permitted where it complies with Human Rights and associated legislation, specifically during an investigation of an allegation of a serious disciplinary offence and will be authorised by the HR Manager as part of the Council's disciplinary procedure.
130. Employee information will only be accessed by those with a business need to know. Any personal information collected in the course of monitoring or surveillance that is not in line with the purposes described above will not be accessed, unless it is required or permitted by law. A form is in place that sets out the detail required for the authorisation, review and cancellation of employee covert surveillance which should only be used in exceptional circumstances and in line with guidance from the ICO.

Non-RIPA surveillance of the public and third parties

131. Paragraph 68 of this policy sets out that in exceptional circumstances the Council will carry out covert surveillance to progress investigations outside of the RIPA framework, where (i) while significant, the matters under investigation may not typically result in criminal proceedings, or (ii) the potential criminal offence(s) under investigation are likely to attract a penalty below the RIPA threshold. The form for this process must be completed and submitted to the SRO for approval before non-RIPA covert surveillance of third parties or the public is conducted.
132. Surveillance under this policy section must be conducted with a view to minimising data collected and minimising the length of time surveillance is conducted for. A maximum of 30 days can be approved at any one time.

Equipment

133. All equipment used by the Council will be fit-for-purpose, inspected and maintained to schedule and produce video and audio footage and images to the appropriate evidential standard.
134. Where CCTV cameras are used covertly as part of an operation to observe a targeted individual or group, the appropriate authorisation must be applied for.
135. Equipment for the purposes of covert surveillance will only be installed when the required authorisations and approvals have been obtained by the case worker, as set out in this policy.
136. Covert surveillance equipment will only be installed in residential premises if prior written permission has been obtained from the householder.
137. Equipment and surveillance logs will be allocated from a central record of equipment, and an appropriate audit trail maintained. Upon cancellation all equipment in use must be removed immediately or else as soon as practicable, since further recordings will amount to unauthorised surveillance.

Evidence handling and records management

138. Evidence gathered during the course of overt and covert surveillance will include electronic and paper files and records, video and audio recordings, photographs and negatives.
139. Material gathered as part of surveillance activities will not be used for any purpose other than that authorised. Where surveillance gathers information that may be relevant to other criminality, the Council may disclose this to appropriate law enforcement agencies, in line with data protection legislation.
140. The Council's privacy notices will set out what personal information services may gather from surveillance activities.
141. Evidence gathered during surveillance will be handled, stored and disseminated safely and securely in line supporting procedures and the Council's retention schedule:
- CCTV images will be retained for 28 days;

- covert surveillance records will be retained for seven years;
- additional records will be retained for CHIS; and
- any material that may be relevant to pending or future litigation will be retained until such litigation is concluded, and thereafter subject to periodic review.

142. Where material is obtained unrelated to the investigation and there is no reason to suspect that it will be relevant to any future litigation, it will be destroyed at the earliest opportunity.

143. The Coordinating Officer (Auditor) will maintain a detailed central record of applications, authorisations, orders, reviews, renewals and cancellations, together with supporting documentation. This will be held in the Council's EDRMS in order to facilitate effective records management across the lifecycle.

Supporting policies, procedures and standards

144. The following supporting procedures and guidance will be made available in support of this policy:

- CCTV Code of Practice
- CCTV Code Assessment Pack
- Covert surveillance procedure
- Fleet vehicle tracking procedure
- Drug and alcohol testing procedure.

145. Each procedure will be subject to impact assessment, including data protection impact assessment, and privacy notices will be updated accordingly.

Monitoring and review arrangements

146. This policy will be reviewed on an annual basis, considered by the appropriate Scrutiny Panel(s) and approved by the Executive. The policy and, where appropriate supporting procedures, will be made available on the Council's Open Data site.

147. Ongoing monitoring will be undertaken by the SPoC (overt surveillance) and the Coordinating Officer (Auditor) (covert surveillance) to ensure organisational compliance with this policy on a live basis. Any issue arising will be reported to the SRO and the Council's Risk Management Group and Corporate Governance Board will be updated as appropriate.

148. The Corporate Affairs and Audit Committee is responsible for oversight of the Council's corporate governance processes. To ensure appropriate oversight of surveillance is maintained, an overview of applications, compliance and trends will be provided to the Committee within an annual report from the SRO.

149. Data relating to the Council's overt and covert surveillance activity (redacted as appropriate) will be published annually on the Council's Open Data site.

150. Statistical returns for CCTV will be submitted to the Surveillance Camera Commissioner by the SRO upon request. The SRO will comply with requests from the Surveillance Camera Commissioner in relation to the organisation of inspections of the Council.

151. Statistical returns for directed surveillance and communications acquired using RIPA will be submitted to the IPCO by the SRO upon request. The SRO will comply with requests from the IPCO in relation to the organisation of inspections of the Council.

Complaints

152. Complaints relating to any surveillance matters must be made in writing and addressed to:

Senior Responsible Officer (Surveillance)
Middlesbrough Council
PO Box 500
Middlesbrough
TS1 9FT

153. Complaints will be investigated in line with the Council's complaints policy and where appropriate the Council's data protection policies. All alleged breaches of privacy will be investigated and appropriate action taken.

154. If the complainant remains dissatisfied following the SRO's response they will if appropriate be advised to write to the Local Government and Adult Social Care Ombudsman and / or the Information Commissioner's Office as appropriate.

155. If the complaint relates to covert surveillance, complainants will also have recourse to:

The Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ
Tel. 0207 035 3711

156. Costs incurred by the Council as a result of cases progressed to The Investigatory Powers Tribunal or the courts, will be met by the relevant Directorate.

Appendix 1: Definitions

Surveillance

Monitoring, observing or listening to persons, their movements, conversations or other activities and communications. Surveillance may be conducted with or without the assistance of a surveillance device and includes the recording of any information monitored, observed or listened to during the course of surveillance.

Overt surveillance

Surveillance that is intentionally and visibly undertaken. General observations made by officers in the course of their duties constitutes overt surveillance. Surveillance by visible cameras e.g. CCTV, body worn cameras and automatic number plate recognition cameras is also overt surveillance and must be appropriately signed.

Covert surveillance

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. There are three types of covert surveillance: directed surveillance, covert human intelligence sources, and intrusive surveillance.

Directed surveillance

Surveillance is directed if it is covert, but not intrusive, and is undertaken for the purposes of a specific investigation or operation and in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation).

Surveillance will not be directed, and therefore will not require authorisation, if it is done 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 to be sought for carrying out the surveillance.

Covert Human Intelligence Source (CHIS)

A person who establishes or maintains a personal or other relationship with a person and:

- covertly uses such a relationship to obtain information or provide access to any information to another person, or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Intrusive surveillance

Surveillance is intrusive if it is covert surveillance that (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Local authorities are not permitted to carry out intrusive surveillance in any circumstances.

Private information

Information capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationship. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public.

Collateral intrusion

The risk of intrusion into the privacy of persons other than the target of covert surveillance.

Confidential information

Consists of matters subject to legal privilege, confidential journalistic material, constituent information and confidential personal information which is held in confidence about the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it.

Residential premises

Any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This includes hotel rooms or rented flats but not communal areas, front gardens, hotel reception areas or dining rooms or driveways readily visible to the public.

Private vehicles

Any vehicle which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This includes leased and company cars.

Communications data

Information about communications: the 'who', 'where' 'when', 'how', and 'with whom' of a communication but not what was written or said (i.e. not content). Generally, it is data that may be acquired from a Telecommunication Operator (TO) as per below.

Entity data (as per the Communications Data Code of Practice 2018)

Data regarding the use of service(s) by customers, including:

- subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;

- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information about selection of preferential numbers or discount calls.

Event data

Identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time, including:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

Local authorities are prohibited from acquiring internet connection records for any purpose.

National Anti-Fraud Network (NAFN)

A not-for-profit public sector organisation providing a range of data and intelligence services that are subscribed to by over 90% of local authorities. NAFN acts as the Council's Single Point of Contact for the acquisition of external communications data, liaising with the Office for Communications Data Authorisations on the Council's behalf.

Office for Communications Data Authorisations (OCDA)

Created under the IPA, the Office for Communications Data Authorisations considers requests for communications data from law enforcement and public authorities.

Surveillance Camera Commissioner

The role of Surveillance Camera Commissioner (Professor Fraser Sampson) was created under POFA to encourage compliance with the surveillance camera code of practice, review how the code is working, and provide advice to ministers on whether or not the code needs amending.

Investigatory Powers Commissioner's Office (IPCO)

Overseen by the Investigatory Powers Commissioner (Sir Brian Leveson), the IPCO was created under the IPA to provide independent oversight and authorisation of the use of investigatory powers by intelligence agencies, police forces and other public authorities.

Appendix 2: Key officers

Senior Responsible Officer (SRO) for both Surveillance and CCTV

Ann-Marie Johnstone, Head of Policy Governance and Information
Deputy: Leanne Hamer, Governance and Information Manager

CCTV Single Point of Contact (SPoC)

Dale Metcalfe, Operational Community Safety Manager

Coordinating Officer (Auditor)

Leanne Hamer, Governance and Information Manager
Deputy: Michael Brearley, Data Protection Officer (for compliance audit purposes only)

Authorising Officers

Richard Horniman, Director of Regeneration and Culture
Judith Hedgley, Head of Public Protection
Paul Clarke, Head of Planning

Authorising officers deputise for one another.

Authorising Officer for Juvenile / Vulnerable Adult CHIS, or where confidential information or matters subject to legal privilege are likely to be acquired through either directed surveillance or by a CHIS

Clive Heaphy, Chief Executive

Designated person

Judith Hedgley, Head of Public Protection
Deputy: Ann-Marie Johnstone, Head of Policy, Governance and Information

Non-RIPA Staff surveillance authorising officer

HR Manager, Kerry Rowe.

Appendix 2: Impact Assessment Level 1: Initial screening assessment

Subject of assessment:	Surveillance Policy 2024/25			
Coverage:	Overarching / crosscutting			
This is a decision relating to:	<input type="checkbox"/> Strategy	<input checked="" type="checkbox"/> Policy	<input type="checkbox"/> Service	<input type="checkbox"/> Function
	<input type="checkbox"/> Process/procedure	<input type="checkbox"/> Programme	<input type="checkbox"/> Project	<input type="checkbox"/> Review
	<input type="checkbox"/> Organisational change	<input type="checkbox"/> Other (please state)		
It is a:	New approach:	<input type="checkbox"/>	Revision of an existing approach:	<input checked="" type="checkbox"/>
It is driven by:	Legislation:	<input checked="" type="checkbox"/>	Local or corporate requirements:	<input checked="" type="checkbox"/>
Page 63 Description:	<p>Key aims, objectives and activities The proposed policy provides a framework for the undertaking surveillance activities across the Council in compliance with all applicable laws by.</p> <p>Statutory drivers Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, UK General Data Protection Regulation, Data Protection Act 2018, Protection of Freedoms Act 2012, Investigatory Powers Act 2016</p> <p>Differences from any previous approach This policy supersedes and subsumes the Council's existing RIPA Policy, setting out the Council's policy in relation to CCTV, non-RIPA surveillance and employee surveillance, amongst other matters.</p> <p>Key stakeholders and intended beneficiaries (internal and external as appropriate) Elected members, employees of the Council, local communities and businesses, partners, regulators.</p> <p>Intended outcomes To ensure that the Council's approach to surveillance clearly articulated and communicated to all stakeholders, and that the Council continues to comply with its legal duties.</p>			
Live date:	December 2024			
Lifespan:	December 2024- December 2025			
Date of next review:	Reviewed on an annual basis.			

Screening questions	Response			Evidence
	No	Yes	Uncertain	
<p>Human Rights</p> <p>Could the decision impact negatively on individual Human Rights as enshrined in UK legislation?</p>	☒	☐	☐	<p>No. The policy is specifically designed to ensure that human rights as identified in national legislation is not contravened when undertaking surveillance activities.</p> <p>Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.</p>
<p>Equality</p> <p>Could the decision result in adverse differential impacts on groups or individuals with characteristics protected in UK equality law? Could the decision impact differently on other commonly disadvantaged groups?</p>	☒	☐	☐	<p>No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. As a result there are no concerns that the actions could have a disproportionate adverse impact on groups or individuals with characteristics protected in national legislation.</p> <p>Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.</p>
<p>Community cohesion</p> <p>Could the decision impact negatively on relationships between different groups, communities of interest or neighbourhoods within the town?</p>	☒	☐	☐	<p>No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on community cohesion.</p> <p>Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.</p>

Screening questions	Response			Evidence
	No	Yes	Uncertain	
<p>Armed Forces Could the decision impact negatively on those who are currently members of the armed forces of former members in the areas of Council delivered healthcare, compulsory education and housing policies?*</p>	☒	☐	☐	<p>No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on this group.</p> <p>Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.</p>
<p>Care leavers Could the decision impact negatively on those who are care experienced?*</p>	☒	☐	☐	<p>No. The policy will ensure a systematic and evidence-based approach to surveillance undertaken in communities and in the workplace. Specific account will be taken in appropriate assessments of community sensitivities. As a result there are no concerns that the proposed plan could have an adverse impact on this group.</p> <p>Evidence used to inform this assessment includes analysis of legislation, statutory and draft statutory guidance and feedback from the IPCO inspection regime.</p>
Assessment completed by:	Ann-Marie Johnstone, Head of Policy, Governance and Information			
Date:	17/10/2024			
Head of Service:	Ann-Marie Johnstone, Head of Policy, Governance and Information			
Date:	17/10/2024			

This page is intentionally left blank