Surveillance Policy

Creator	Author(s)	Ann-Marie Johnstone Leanne Hamer		
	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	20251111		
	Submitted	20251218		
	Approved	TBC		
	Updating Frequency	Annually, unless review triggers met in interim		
Status	Version: 10.0			
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
8.0	2023/11	Review	L Hamer
9.0	2024/11	Review	AM Johnstone
10.0	2025/11	Review	L Hamer

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
10.0	2025/12	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.

Context

3. This Policy links to HR related policies as surveillance involves monitoring employees and handling personal data. These connections include:

    - Data Protection Policy,
        i. Collection of personal data (e.g. CCTV footage)
    - Wider IT Security Policies
        i. If surveillance includes monitoring emails, internet usage or devices, this links to ICT policies
    - Disciplinary Policy
        i. Ensuring fairness and transparency in disciplinary processes
    - Health & Safety Policy
        i. CCTV or monitoring used for safety purposes , assurance this aligns with duty of care obligations
    - Equality & Inclusion Policy
        i. Not discriminating or disproportionately targeting certain groups
        ii. Checks on compliance with equality legislation

Purpose

4. 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 respect for private and family life (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

5. 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

6. 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.

7. Currently the Council does not use drones for surveillance or enforcement purposes.

8. 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, other sanction for employees or for other parties enforcement in relation to the terms and conditions of the contract.

9. 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.

10. 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

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

Human Rights Act 1998

12. The Human Rights Act 1998 (HRA) gave effect in UK law to the rights set out in the European Convention on Human Rights (EHCR).

13. 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.

14. 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

15. 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 EHCR and the Data Protection Act 2018.

16. 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.

17. The grounds on which local authorities can rely 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.

18. 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.

19. 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.

20. 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

21. 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.

22. 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.

23. 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.

24. 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.

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

Protection of Freedoms Act 2012

26. 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.

27. 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.

28. 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

29. 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.

30. 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

31. 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.

32. 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

33. 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 HRA 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

Policy detail

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

Overt surveillance

35. 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.

36. 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.

37. The SRO will appoint a SPoC for CCTV and notify the Surveillance Camera Commissioner accordingly.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

43. 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.

44. 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

45. 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

46. The Council will use covert surveillance to acquire information to support investigations where it is lawful and appropriate to do so.

47. 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.

48. 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.

49. 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.

50. 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.

51. Both RIPA and non-RIPA surveillance will use a systematic process of:

    - application;
    - authorisation;
    - conduct of authorisation;
    - review;
    - renewal (where necessary); and
    - cancellation.

52. 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

53. 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.

54. 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.

55. 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.

56. 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.

57. 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

58. 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.

59. 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.

60. 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.

61. The authorising officer will notify the applicant and the Coordinating Officer (Auditor) of the decision reached.

62. 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.

63. 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.

64. 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.

65. Written authorisations for non-RIPA applications will be considered by the SIRO as authorising officer.

Conduct of authorisation

66. 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.

67. 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.

68. 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

69. 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.

70. The applicant will send the completed form to the relevant authorising officer and the coordinating officer.

Renewal

71. 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.

72. 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.

73. If the authorisation lapses during this period then no further surveillance can be undertaken until the JP has approved the renewal for RIPA applications.

74. 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.

75. For non-RIPA applications, renewal applications for surveillance will be considered by the SIRO as authorising officer.

Cancellation

76. There is a presumption that covert surveillance or CHIS authorisations (RIPA only) will be cancelled at the earliest opportunity using the appropriate form.

77. 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.

78. Authorisations must also be cancelled when the authorisation period has expired and a renewal has not been requested and authorised.

79. The applicant will send the completed form to the relevant authorising officer and the coordinating officer.

Errors

80. 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)

81. 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.

82. Individuals contacting the Council to provide unsolicited information on a one-off basis will not be considered CHIS.

83. 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.

84. 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.

85. 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

86. 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.

87. 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.

88. 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

89. 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.

90. 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.

91. 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

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

93. 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.

94. 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.

95. 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.

96. 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.

97. 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

98. 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.

99. 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.

100. 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]

101. 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.

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

103. 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.

104. 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.

105. 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.

106. 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.

107. 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).

108. 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.

109. 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.

110. Routine monitoring of systems access will be undertaken to ensure that employee access to customer personal data is lawful and appropriate.

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

111. 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.

112. 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

113. 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.

114. 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

115. 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.

116. 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.

117. 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.

118. Covert surveillance equipment will only be installed in residential premises if prior written permission has been obtained from the householder.

119. 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

120. 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.

121. 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.

122. The Council's privacy notices will set out what personal information services may gather from surveillance activities.

123. 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.

124. 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.

125. 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.

Roles and Responsibilities

126. 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.

127. 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.

128. 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)

129. 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;
- 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

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

CCTV Single Point of Contact (SPOC)

131. 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.

132. 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

133. 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

134. 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

135. 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

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

Coordinating Officer (Auditor)

137. 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

138. 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.

139. 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.

140. 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.

141. 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)

142. 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)

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

Applicants (Case Officers)

144. 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.

Supporting policies, procedures, and standards

145. 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.

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

Monitoring and review arrangements

147 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.

148 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.

149 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.

150 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.

151 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.

152 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

153 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

154 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.

155 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.

156 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

157 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)

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

CCTV Single Point of Contact (SPoC)

John Kirk, Service Delivery 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
Claire Holt, Head of Strategic Housing

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

Louise Grabham, Director of Adult Social Care and Public Health

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.