Meeting of:	**Cabinet**
Date of Meeting:	**Thursday, 06 February 2025**
Relevant Scrutiny Committee:	Corporate Performance and Resources
Report Title:	Surveillance and the Regulation of Investigatory Powers Act 2000
Purpose of Report:	To provide Cabinet with an updated Policy regarding surveillance
Report Owner:	Executive Leader and Cabinet Member for Performance and Resources
Responsible Officer:	Tom Bowring, Director of Corporate Resources
Elected Member and Officer Consultation:	Due to the corporate nature of this report, no ward Member consultation has been undertaken. Consultation activities with staff are described within the body of the report.
Policy Framework:	This is a matter for Executive decision by Cabinet.

Executive Summary:

- The Council as part of its functions undertakes surveillance on occasion, some of which may be covert. In order to ensure good practice and that the Council operates legally and fairly, balancing evidence gathering and individual rights appropriately, the Council has a number of factors in place. This includes an overarching policy, which sets out the Council's expectations and the Council's governance arrangements.
- The Council's policy is subject to review in order to ensure that it remains relevant and current to the latest legislation and the operations of the Council. The policy is subject to review by Cabinet. The then Leader of the Council last considered the policy in 2020,during the pandemic.
- Since 2020, the Council has appointed a new Information Governance Manager and Monitoring Officer. Both roles play a key part in the oversight of these activities. A review of the Council's policy has taken place. The amendments reflect changes in the law and ensure future resilience in oversight of these activities.
- Details of the amendments are set out in this report together with information relating to the Council's other initiatives in this area, which seek to ensure officers are aware of the policy and their responsibilities when carrying out surveillance.

Recommendations

1. That Cabinet notes the contents of this report and the updated policy (Appendix A).
2. That, subject to Recommendation 1, Cabinet endorses the updated policy (Appendix A).

Reasons for Recommendations

1. To enable Cabinet to consider and note the updated policy.
2. To ensure the Council has an up-to-date policy, supported by the Council's Executive.

1. Background

1.1 The Council like a number of other public organisations or organisations in general may carry out surveillance from time to time. Surveillance can trigger a number of different legal considerations dependent upon its type and nature.

1.2 The legal framework around this area are set out within the policy itself and include the Regulation of Investigatory Powers Act 2000 (RIPA), the Human Rights Act 1998 (HRA) and the Investigatory Powers Act 2016 (IPA). The Data Protection Act 2018 (DPA) is also relevant.

1.3 As part of its public functions the Council undertakes a number of regulatory activities for public safety, examples include environmental health, planning and licensing. In order for these to operate effectively and for the public good sometimes it is necessary for monitoring to be undertaken. The Council can undertake certain types of monitoring/surveillance activity as part of its public functions and these can be covert. Such activity is regulated and can need external approval. It is a powerful tool, for responsible use only.

1.4 The Council may also undertake activities that are considered as surveillance in other situations either covertly or overtly for example within the context of viewing CCTV or monitoring Social Media. In such circumstances, careful consideration is required always to include an individual's right to privacy and private life.

1.5 In order to ensure that the Council undertakes surveillance responsibly and legally, the Council has a number of different mechanisms to support.

1.6 These mechanisms include training, guidance and communication campaigns. The Council endeavours to keep awareness and understanding in place via regular training. The Council's iDEV provides online training in relation to the Regulation of Investigatory Powers Act (RIPA). There is a dedicated page on Staffnet to assist officers with surveillance. Regular training is provided, both virtually and in person. In addition to the online support, in October 2023, Senior Leadership Team members and officers participated in training which focussed

upon surveillance and the application of the Regulation of Investigatory Powers Act 2000 and the Human Rights Act. During 2024 preparatory work in updating the policy, guidance training and general information available has been undertaken. This has culminated in the updated policy.

1.7 In addition to the policy, guidance has been updated and the iDEV training updated. A communications campaign to raise awareness and update officers generally has been progressed in January 2025.

2. Key Issues for Consideration

2.1 The updated policy content structure, attached at Appendix A, remains the same. The language and detail within the policy has been reviewed in an attempt to make it more "user friendly". The nature of the relevant legislation is complex. The primary focus of the policy is to set out the Council's expectations and its governance arrangements. Internally within the organisation it is the starting point when considering undertaking surveillance.

2.2 There has been a change in the law, within Part I of RIPA, since the last iteration of the policy, which deals with communications, as amended by the Investigatory Powers Act 2016. The updated policy reflects those changes.

2.3 The number of nominated authorising officers has been increased in order to ensure there is adequate resilience and capacity. The increase is also to ensure that the likelihood of a conflict arising can be negated.

2.4 The amended policy includes a requirement to review the policy every two years.

3. How do proposals evidence the Five Ways of Working and contribute to our Well-being Objectives?

3.1 The policy forms part of the Council's integrated planning with specific focus on aligning these practices with the Well-being duties under the Well-Being of Future Generations (Wales) Act 2015. The Regulation of Investigatory Powers Act 2000 governs the use of covert surveillance by public bodies, including local authorities, to ensure that such activities are conducted lawfully. The Well-being of Future Generations Act mandates public bodies to work towards improving the social, economic, environmental, and cultural well-being of Wales and its citizens, emphasising sustainable development and long-term thinking. The Policy in contributing to all four Well-being Objectives, ensures the long-term impact on individual privacy; emphasises preventative measures in surveillance in contributing to a healthier and more cohesive community; enhanced collaboration between public bodies, ensuring a more integrated to surveillance and well-being.

4. Climate Change and Nature Implications

4.1 The Policy enables work to be undertaken that supports departments in meeting these implications. For example surveillance can be used where there are concerns of illegal dumping of waste and illegal planning activity.

5. Resources and Legal Considerations

Financial

5.1 There are no direct financial implications arising from this policy. A failure to adhere to the policy could lead to a financial implication if the Council were found to be operating contrary to the legislative framework in place for surveillance activity.

Employment

5.2 There are no employment implications arising as a direct result of this report.

Legal (Including Equalities)

5.3 There are no direct legal implications arising from this report and are as set out in the body of this report and the policy itself.

6. Background Papers

None.

SURVEILLANCE AND THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1 Introduction

1.1 As part of its public functions the Council undertakes a number of regulatory activities for public safety, examples include environmental health, planning and licensing. In order for these to operate effectively and for the public good sometimes it is necessary for monitoring to be undertaken.

1.2 The Council is able to undertake certain types of monitoring/surveillance activity as part of its public functions and these can be covert. Such activity is a powerful tool, for responsible use only.

1.3 This policy seeks to set out the Council's position and its expectations of Officers as well as explaining the Council's internal arrangements for dealing with surveillance, in conjunction with the law around this area. The ultimate aim of this policy is to ensure good practice throughout the Council, striking an appropriate balance between evidence gathering and individual rights.

1.4 In addition to this policy, the Council also has other sources of information, which should be considered. This includes a separate guidance document: "Monitoring in the course of your employment and as part of your duties. RIPA and beyond" and the Codes of Practice. Details of the further information available to staff and access to the Codes of Practice can be found on the Council's internal staff net pages.

2 Policy

2.1 The Council accepts that it has extensive powers and that it must use them responsibly. Consideration of all alternative options must take place firstly. The use of surveillance in any form should be the best/only option. There must be a legitimate objective.

2.2 The Council can and will only use the powers granted where it is allowed to do so in law. The Council recognises that it is vital that only appropriate and experienced staff are able to use these powers. They must have undertaken relevant training and have easy access to information and guidance.

2.3 The Council also recognises that it is important for all staff to have an awareness around this topic and that there must be clear procedures in place so that the system is effectively managed.

3 Legal Framework

3.1 The Human Rights Act 1998 ('HRA') makes it unlawful for the Council to act in any way that is incompatible with the rights set out in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

3.2 Human rights are needed to protect and preserve every individual's

humanity, to ensure that every individual can live a life of dignity. The Convention sets out a number of rights. Particularly relevant in this area are the right of respect for private and family life and the right to a fair trial.

3.3 The Council must consider the HRA when conducting all of its activities whether it involves citizens, Elected Members, employees, or other third parties.

3.4 Surveillance can also trigger individual rights under the Data Protection Act (DPA).

3.5 RIPA, (The Regulation of Investigatory Powers Act 2000), introduced a system of authorisations, which serves to secure the lawfulness of covert surveillance activities where there is a suspicion of certain illegal or criminal activities. It also ensures they are consistent with the Council's obligations under HRA. Such activity can breach a person's human rights. RIPA seeks to avoid this from happening. It provides the legal framework to ensure activities are necessary, proportionate and lawful. RIPA applies to a wide range of criminal investigations such as terrorism, crime, public safety and emergency services.

3.6 Local authorities have a wide range of functions and are responsible in law for enforcing over 100 separate Acts of Parliament. In particular local authorities investigate offences in the following areas:

- trading standards, including action taken against loan sharks and rogue traders, consumer scams, sale of counterfeit goods, unsafe toys and electrical goods;

- environmental health, including action against large-scale waste dumping, dangerous workplaces, pest control and the sale of unfit food;

- benefit fraud, including action to counter fraudulent claims for housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations and council tax evasion.

3.7 The Council is always accountable for its actions. In some instances of surveillance type activity RIPA may not apply. This can arise because the criminal penalty threshold is not met or because it relates to a civil matter such as social services or employment. In these situations, the Council still must consider the appropriateness of its actions and be mindful of an individual's Human Rights. The Council has a separate process for such situations, and it must be used.

3.8 A failure to comply with the Council's policy or guidance and/or the Codes of Practice can leave the Council vulnerable to action being taken against it such as in the Investigation Powers Tribunal. It can damage the progression of legal processes such as prosecutions or other legal matters. It can also cause reputational damage. For individuals if there is a failure to follow Council Policy, guidance or the Codes of Practice then disciplinary action may be considered.

Part I of RIPA

3.9 Part I of RIPA relates to the interception of Communications Data. The Investigatory Powers Act 2016 has amended most of those aspects of RIPA as relevant to communications data within Part I of the Act.

3.10 Acquisition of Communications data is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written).

3.11 Communications data is categorised as: -

I. Events data which identifies or describes events which consist of one or more entities engaging in an activity at a specific time or times.

II. Events data refers to both Traffic data (which includes information about where the communications are made or received) is classed as an intrusive type of data; and Service use information (such as the type of communication, time sent and its duration).

III. Entity Data / Subscriber information (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services)

the second and third examples above are not classed as intrusive types of communications data.

Where the purpose of the acquisition is to prevent or detect crime, and the data required is events data, the offence or conduct of the offence being investigated must meet at least one of the definitions of serious crime.

3.12 The Council is involved in everyday functions of law enforcement. In some instances, it may be necessary to use communications data as part of their enforcement function.

For example: -

Trading Standards might use communications data to discover the name and address of the subscriber of a telephone number identified in their operations who is suspected to be an illegal money lender. Food Hygiene inspectors may wish to ascertain the identity of illegal food suppliers.

Council Officers normally use communications data to identify the operators of businesses that have committed, or is suspected of committing, a crime when other investigation techniques have been unsuccessful.

3.13 It is illegal for Local Authorities to intercept the content of any person's communications without lawful authority. It is an offence to do so.

3.14 Surveillance under Part I of the Act and the Investigatory Powers Act 2016 (IPA) are not subject to the crime threshold as applies in Part II (see below). Some elements are subject to **a serious crime test**. For the serious crime test to be met it must be one of the following: -

I. An offence that is capable of attracting a prison sentence of 12 months or more

II. An offence by a person who is not an individual (i.e. a corporate body)

III. An offence falling within the definition of serious crime in section 81(3)(b) of the Act (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of person in pursuit of a common purpose)

IV. An offence which involves, as an integral part of it, the sending of a communication

V. An offence which involves, as an integral part of it, a breach of a person's privacy

3.15 But there is no power to intercept communications in the course of communication.

3.16 The Council can only acquire and disclose communications data for the purposes of preventing or detecting crime or preventing disorder.

3.17 The procedure for Part I activities differs from Part II.

3.18 The Office for Communications Data Authorisations (OCDA) assesses Communications Data applications, these types of application no longer require judicial approval.

3.19 Under the IPA, OCDA are responsible for ensuring that any applications made by relevant authorities in the UK are assessed independently and rigorously. The OCDA acts as a hub of authorisation expertise, independently assessing applications, holding authorities accountable to robust safeguarding standards, and challenging where required.

3.20 Local authorities must submit all their communication data applications via an Accredited Officer known as a Single Point of Contact (SPoC) who has passed a Home Office approved course. All Councils must use the National Anti-Fraud Network (NAFN) as their SPoC. Therefore, all applications to access Communications Data are made through NAFN via their online application service. All applications must be authorised by OCDA prior to any communications data being acquired on behalf of a Local Authority.

3.21 Internally, prior to the submission to NAFN an Authorising Officer (AO) must have considered the application, which is proposed, the Information Governance Manager (IGM) must be consulted, and the Senior Responsible Officer (SRO) must be aware of it.

3.22 There is a separate Code of Practice for Communications Data and Officers working in this area must have regard to it:

https://www.gov.uk/government/publications/communications-data-code-of-practice

3.23 Further detailed information can also be found in the Council's "Guidance for Officers – Monitoring in the course of your employment and as part of your

duties. RIPA and beyond.

Part II of RIPA

3.24 Part II of RIPA provides for authorisation of Covert Surveillance by Local Authorities where that surveillance is likely to result in the obtaining of private information about a person (Directed Surveillance). It also provides for the authorisation of the use or conduct of a Covert Human Intelligence Source (CHIS).

3.25 Surveillance is defined within RIPA, and it includes: -

I. monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

II. recording anything monitored, observed or listened to in the course of surveillance; and

III. surveillance by or with the assistance of a surveillance device.

3.26 RIPA also defines Covert Surveillance. It is defined as: -

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

3.27 A person is a CHIS if:

(a) *He establishes or maintains a personal or other relationship with the person for the covert purpose of facilitating or doing anything falling within paragraphs (b) or (c)*

(b) *He uses such a relationship to obtain information or provide access to information to another person or*

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

3.28 In order to conduct surveillance under Part II of the Act as highlighted above, it is necessary to obtain internal authorisation via an AO and with overview of a SRO and with Judicial Approval. RIPA under Part II requires a Justice of the Peace /Magistrate (JP) to authorise the surveillance. This involves attending Court and explaining to a JP why the Council wants to carry out the surveillance and the reasons why. Internal authorisation on its own will not be sufficient and it is illegal to carry out surveillance covered by Part II of RIPA without permission from a JP. Further details of how to undertake this process are set out in the Council's guidance Monitoring in the course of your employment and as part of your duties. RIPA and beyond and the

Codes of Practice.

4 Where RIPA does not apply

4.1 In some situations, RIPA will not apply normally because it does not meet the tests such as the criminal threshold or because it is outside scope altogether such as an employment or social services matter. In these situations, the Council expects very careful of consideration of any proposed activity and absolute certainty that surveillance is necessary. In this, instance the Council has a separate non-RIPA process that requires similar questions to be asked and for it to be signed off by an AO and the SRO to be aware.

5 Selection and Training of Personnel

5.1 All Chief Officers across the Council are required to ensure that only appropriate officers with sufficient experience are involved in these activities.

5.2 All Chief Officers across the Council are required to ensure that they know what activities of this nature are being undertaken and that the proper processes and authorisations have been obtained.

5.3 All Officers working in this area must undertake appropriate training.

5.4 All Officers must comply with the provisions of the legislation and supplemental Codes of Practice and guidance in the exercise of powers.

5.5 All Officers must adhere to this policy, all other Council guidance and Codes of Practice. A failure to comply with the Council's Policy and Guidance may place the Council at risk of enforcement action and can lead to disciplinary processes being engaged against individual Officers.

6 Codes of Practice, Legislation, Guidance and Home Office forms

6.1 The current Codes of Practice are available to staff on the Council's Staff-net together with a copy of the primary legislation. Adherence to the Codes is essential. Officers also need to be mindful of the potential for the HRA and DPA to be applicable and must have regard.

6.2 **Prior** to conducting any investigation, Officers should ensure they consider the nature of any proposed activity and the appropriateness of any proposed action. They should be clear as to how their proposed action fits within this policy and ensure that their actions are compliant with this policy, the Council's guidance and policies on all aspects and the Codes of Practice.

6.3 If an Officer is unsure in any way about any activity they are about to embark upon they should contact the Information Governance Manager (IGM) for support and advice before proceeding.

7 Nominated Authorising Officers (AOs)

7.1 The following Officers within the Council are the AOs: -

- Chief Executive
- Head of Finance/ Section 151 Officer,
- Head of Audit
- Director of Place
- Head of Sustainable Development
- Director of Environment & Housing
- Head of Shared Regulatory Service

8 Management of the System

8.1 The SRO is responsible for the following.

- The integrity of the processes in place within this Council dealing with the authorising of directed surveillance, the use of covert human intelligence sources and the accessing of communications data
- Compliance with all relevant statutory provisions and associated guidance
- Having overview of all applications for authorisation
- Engagement with Regulators, Commissioners and Inspectors as necessary including inspections and reference to any specific application as appropriate.
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.
- Ensuring that all AOs are of an appropriate standard in the light of any re-inspection reports prepared by the Office of the Surveillance Commissioner

8.2 The Council's IGM will retain the central record of all decisions of the OCDA under part I of the Act and all applications, reviews, renewals and cancellations in respect of Part II of the Act.

9 Oversight

Elected Members via the Council's Cabinet have strategic oversight of this policy. In particular, they will set policy and approve the management and accountability framework. The system is subject to external oversight from the relevant Commissioners and individual applications are subject to judicial approval or OCDA.

10 Procedure

10.1 Applications in relation to communications or covert surveillance or the use of CHIS are separate and distinct. There are separate Codes of Practice and separate processes for them.

10.2 The IGM must be consulted on all applications, and they must be

submitted to the Council's IGM as the IGM undertakes a gatekeeping role. The IGM maintains a record of the application and the process. The IGM will communicate with the AO. The IGM will also make the SRO aware and will provide support during the process.

10.3 Detailed guidance has been prepared and they are accessible to all Officers on the Council's Staff-net. Officers should make themselves familiar with them, compliance with the procedures and the legislation / Codes of Practice are mandatory.

11 Review

This policy is subject to review by Cabinet at regular intervals, not less than every 2 years.

Updated Policy

Last reviewed January 2025