Nuneaton and Bedworth Borough Council
Town Hall, Coton Road, Nuneaton
Warwickshire CV11 5AA

www.nuneatonandbedworth.gov.uk
024 7637 6376

Enquiries to:
Democratic Services

Direct Dial: 024 7637 6204

Direct Email:
committee@nuneatonandbedworth.gov.uk

Date: 17th July 2024

INDIVIDUAL CABINET MEMBER DECISION

Dear Sir/Madam,

The Cabinet Member for Resources and Customer Service (Councillor S. Hey) is to consider the following reports and make a decision on **Tuesday, 6 August 2024** at **11.30am** in Committee Room D, Town Hall, Nuneaton.

Yours faithfully,

TOM SHARDLOW

Chief Executive

A G E N D A

PART 1

PUBLIC BUSINESS

1. EVACUATION PROCEDURE

A fire drill is not expected, so if the alarm sounds, please evacuate the building quickly and calmly. Please use the stairs and do not use the lifts. Once out of the building, please gather outside Lloyds Bank on the opposite side of the road.

Exit by the door by which you entered the room or by the fire exits which are clearly indicated by the standard green fire exit signs.

If you need any assistance in evacuating the building, please make yourself known to a member of staff.

Please also make sure all your mobile phones are turned off or set to silent.

2. PUBLIC CONSULTATION - Members of the public will be given the opportunity to speak on specific agenda items if notice has been received.

Members of the public will be given three minutes to speak on a particular item and this is strictly timed. The chair will inform all public speakers that: their comments must be limited to addressing issues raised in the agenda item under consideration: and that any departure from the item will not be tolerated.

The chair may interrupt the speaker if they start discussing other matters which are not related to the item, or the speaker uses threatening or inappropriate language towards Councillors or officers and if after a warning issued by the chair, the speaker persists, they will be asked to stop speaking by the chair. The chair will advise the speaker that, having ignored the warning, the speaker's opportunity to speak to the current or other items on the agenda may not be allowed. In this eventuality, the chair has discretion to exclude the speaker from speaking further on the item under consideration or other items of the agenda.

3. DECLARATIONS OF INTEREST - To receive declarations of Disclosable Pecuniary and Other Interests, in accordance with the Members' Code of Conduct.

Declaring interests at meetings

If there is any item of business to be discussed at the meeting in which you have a disclosable pecuniary interest or non- pecuniary interest (Other Interests), you must declare the interest appropriately at the start of the meeting or as soon as you become aware that you have an interest.

Arrangements have been made for interests that are declared regularly by members to be appended to the agenda **(Page 4).** Any interest noted in the Schedule at the back of the agenda papers will be deemed to have been declared and will be minuted as such by the Committee Services Officer. As a general rule, there will, therefore, be no need for those Members to declare those interests as set out in the schedule.

There are, however, TWO EXCEPTIONS to the general rule:

1. When the interest amounts to a Disclosable Pecuniary Interest that is

engaged in connection with any item on the agenda and the member feels that the interest is such that they must leave the room. Prior to leaving the room, the member must inform the meeting that they are doing so, to ensure that it is recorded in the minutes.

2. Where a dispensation has been granted to vote and/or speak on an item where there is a Disclosable Pecuniary Interest, but it is not referred to in the Schedule (where for example, the dispensation was granted by the Monitoring Officer immediately prior to the meeting). The existence and nature of the dispensation needs to be recorded in the minutes and will, therefore, have to be disclosed at an appropriate time to the meeting.

Note: Following the adoption of the new Code of Conduct, Members are reminded that they should declare the existence and nature of their personal interests at the commencement of the relevant item (or as soon as the interest becomes apparent). If that interest is a Disclosable Pecuniary or a Deemed Disclosable Pecuniary Interest, the Member must withdraw from the room.

Where a Member has a Disclosable Pecuniary Interest but has received a dispensation from Audit & Standards Committee, that Member may vote and/or speak on the matter (as the case may be) and must disclose the existence of the dispensation and any restrictions placed on it at the time the interest is declared.

Where a Member has a Deemed Disclosable Interest as defined in the Code of Conduct, the Member may address the meeting as a member of the public as set out in the Code.

Note: Council Procedure Rules require Members with Disclosable Pecuniary Interests to withdraw from the meeting unless a dispensation allows them to remain to vote and/or speak on the business giving rise to the interest.

Where a Member has a Deemed Disclosable Interest, the Council's Code of Conduct permits public speaking on the item, after which the Member is required by Council Procedure Rules to withdraw from the meeting.

4. POLICY DOCUMENTS – report of the People Services Manager, attached **(Page 5).**

Schedule of Declarations of Interests – 2024/2025
Councillor S. Hey

	Name of Councillor	Disclosable Pecuniary Interest	Other Personal Interest	Dispensation
	General dispensations granted to all members under s.33 of the Localism Act 2011			Granted to all members of the Council in the areas of: - Housing matters - Statutory sick pay under Part XI of the Social Security Contributions and Benefits Act 1992 - An allowance, payment given to members - An indemnity given to members - Any ceremonial honour given to members - Setting council tax or a precept under the Local Government Finance Act 1992 - Planning and Licensing matters - Allotments - Local Enterprise Partnership
	S. Hey	Director – - Heywire Ltd - Brilliant Bookings Ltd	Member of the Labour Party, National Trust, CAMRA (Campaign for Real Ale), Royal Photographic Society. Representative on the following Outside Bodies: • West Midlands Employers Board (NBBC representative) • Local Government Superannuation Scheme Consultative Board • Grayson Place (NBBC) Limited • West Midlands Employers • Nuneaton and Bedworth Older People's Forum	

Nuneaton & Bedworth
United to Achieve

Agenda item: 4

Individual Cabinet Member Decision

Report Summary Sheet

Date:	06 August 2024
Subject:	Policy Documents
Portfolio:	Finance and Corporate [Cllr S. Hey]
From:	Ruth Bartlett – People Services Manager

Summary:	To seek approval of a number of Policy Documents.
Recommendations	1. That the following documents be approved: • Regulation and Investigatory Powers Act - Guidance and Procedure (Appendix A) • Policy in Relation to Monitoring and Surveillance in the Workplace (Appendix B)
Reasons:	To ensure that the Council complies with legislation and good practice by providing clear, concise and up to date Policy documentation to assist consistency across the Council. To ensure policies accurately reflect recent changes in structure, personnel and responsibilities.
Options:	1. Accept the recommendations 2. Approve some documents. This may result in the Council not complying with employment legislation and good practice which may produce inconsistency in approach across the Council 3. Not approve any of the documents. This may also result in the Council not complying with employment legislation and good practice which may produce inconsistency in approach across the Council

Subject to call-in:	Yes
Forward plan:	No
Corporate priorities:	Aim 4 priority 3
Relevant statutes or policy:	General Legislation

Equalities Implications:	All Council policies must have a consistent approach to allow the inclusion of all of. An equalities impact assessment has been undertaken and the recommended amendments have been made. This process ensures that there are no inequalities by the introduction of the documentation.
Human Resources Implications:	The provision of the Policy documentation will assist consistency in approach across the Council.
Financial Implications:	None identified
Health Inequalities Implications:	None identified
Section 17 Crime & Disorder Implications:	None identified
Risk Management Implications:	If not approved, there is a risk that the Council may not be compliant with current legislation
Environmental Implications:	None identified
Legal implications:	If not approved, there is a risk that the Council may not be compliant with current legislation

Contact details:	Ruth Bartlett, People Services Manager Tel.No.:02476376211 Ruth.bartlett@nuneatonandbedworth.gov.uk

Agenda Item No. 4

NUNEATON AND BEDWORTH BOROUGH COUNCIL

Report to:	**Individual Cabinet Member Decision**
Date:	**06 August 2024**
From:	**Ruth Bartlett, People Services Manager**
Subject:	**Policy Documents**
Portfolio:	**Finance and Corporate [Cllr S. Hey]**

---

1. Purpose of Report

1.1 To seek approval of a number of Policy Documents.

2. Recommendation

2.1 That the Committee note the report; and

2.2 That the following documents be approved:

- Regulation and Investigatory Powers Act - Guidance and Procedure (Appendix A)
- Policy in Relation to Monitoring and Surveillance in the Workplace (Appendix B)

3. Background

3.1 The development and review of policy documentation provides a framework to assist in a consistent approach across the Council and enhance the equalities agenda. An equalities impact assessment has been undertaken to assess the potential equalities impact the policy documentation may have upon the workforce.

3.2 The provision of good quality documentation promotes and develops good Employee Relations with Trade Union Representatives.

4. Policy Documents

4.1 Regulation and Investigatory Powers Act - Guidance and Procedure

4.1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a legal framework for surveillance and information gathering techniques undertaken by public bodies in the course of their duties.

4.1.2 In the main, changes are minor as the policy continues to reflect current legislation. However, updates have been made to reflect roles and responsibilities applicable to this policy given the recent revised management restructure.

4.2 Policy in Relation to Monitoring and Surveillance in the Workplace

4.2.1 This policy is newly developed and aims to compliment the policy noted in 4.1 in providing guidance for managers and employees in relation to various processes and tools in use that may capture data and information in the workplace.

4.2.2 In an ever increasing digital world, the policy provides information about these processes and tools and how the information may be used to monitor the workplace, in the main to ensure efficient services and safety and welfare of employees.

5. Consultation

5.1 Appropriate consultation has been undertaken with the Council's Management Team and the relevant Trade Union Representatives. Furthermore, this report and the policy documents have been brought to the attention of all staff so that they may make any comments or views.

6. Conclusion

6.1 The Council regularly produces, reviews and amends policy documentation where necessary to conform to changes in legislation and best practice.

6.2 The provision of appropriate Strategies, Policies and Procedures will assist consistency across the Council and promote good Employee Relations with the Trade Unions.

APPENDICES

- Regulation and Investigatory Powers Act - Guidance and Procedure (Appendix A)
- Policy in Relation to Monitoring and Surveillance in the Workplace (Appendix B)

APPENDIX A

Nuneaton & Bedworth

Regulation of Investigatory Powers Act 2000

Guidance and Procedure Document

Covert Surveillance

Date	Responsibility	Approved
1st December 2022	Director – Planning and Regulation	Approved
~~XXXXX~~ 15th July 2024	Assistant Director – Democracy and Governance	Draft

INDEX

1. INTRODUCTION

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a legal framework for surveillance and information gathering techniques undertaken by public bodies in the course of their duties. Such activity must be consistent the Human Rights Act 1998 (HRA) which provides that *"Everyone has the right to respect for his private and family life, his home and his correspondence" (Art 8)*

Most investigatory or enforcement activity carried out by the Council will be carried out in an open or overt manner. However, on occasion, officers may need to undertake their duties in a covert manner. Covert surveillance is surveillance, carried out so that the people being observed, or listened to, or monitored, are unaware that it is, or may be, taking place.

This document is intended to cover the surveillance and information gathering techniques which are most appropriate to local authority work, such as environmental health, planning and internal audit.

RIPA aims to ensure that when public bodies carry out investigations:

- *they respect the privacy of individuals and*
- *that there is an interference with privacy only where the law permits it and*
- *there is a clear public interest justification.*

RIPA provides that covert surveillance will be lawful if an authorisation has been properly issued and a person acts in accordance with that authorisation.

In authorising surveillance, the Council must be satisfied that:

- *Any surveillance is undertaken in connection with a statutory function with which the Council is charged.*
- *That such interference can be justified legally.*
- *The surveillance is properly authorised in accordance with this policy and consequently provides a basis for justifying any interference with a person's human rights*

Local authorities are restricted in the type of surveillance and information gathering techniques which they can be authorised to undertake under RIPA.

- **directed surveillance**
- **the use of covert human intelligence sources (CHIS)**
- **acquisition of communications data**.

All directed surveillance, use of a CHIS or accessing communications data must be properly authorised.

Following changes to RIPA by the Protection of Freedoms Act 2012, the Council can only authorise directed surveillance for the purpose of preventing or detecting more serious criminal offences which attract a custodial sentence of six months or more., Local Authority authorisations must also now be approved by a Magistrate.

Failure to obtain an authorisation is likely to be deemed to be unlawful under the HRA and evidence gathered is liable to be ruled inadmissible in Court, with costs being awarded against the Council and complaints made.

RIPA authorisation cannot be sought for low level offences such as dog fouling or fly posting which do not meet the serious crime threshold, however the principles in this policy should be applied to

any surveillance activity falling below the threshold (non-RIPA activity) and the Council's Internet and Social Media Investigation Procedure (February 2022) should be adhered to.

Reference Documents

The Home Office has issued Codes of Practice including:
• Covert surveillance and property interference (2014, updated 2018)
• Covert human intelligence sources (2014, updated 2018)
• Acquisition and disclosure of communications data (2015)
• Interception of communications (2016).
These and other relevant guidance are available at:
https://www.gov.uk/government/collections/ripa-codes

The Act provides for oversight arrangements as follows:

Investigatory Powers Commissioner and Tribunal

The Government has appointed the Investigatory Powers Commissioner to review how public authorities implement the requirements of RIPA. The Commissioner has wide ranging powers of access and investigation. The Council receives periodic visits from the Commissioner's staff and therefore it is essential that everyone who engages in covert surveillance is fully aware of the law and this procedure. In addition the Act establishes a Tribunal made up of senior members of the judiciary and the legal profession which is independent of the Government. The Tribunal has full powers to investigate and decide any case where a complaint is made about the conduct of the Council in exercising its surveillance powers.
For further information see

http://www.ipco.org.uk

Details of the relevant complaints' procedure can be obtained from the following address:
Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ
020 7273 4514

2. WHAT IS COVERT SURVEILLANCE?

RIPA defines surveillance as:

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

Covert Surveillance is surveillance carried out so that the people being observed, or listened to or monitored are unaware that it is or may be taking place

There are two categories of **covert surveillance**:

- Directed Surveillance, and
- Intrusive Surveillance

Directed Surveillance

Directed Covert Surveillance (DCS) is defined as surveillance which is covert, but not intrusive, and undertaken:

kkkkk) for the purpose of a specific investigation or operation;

llll) in such a manner as is likely to result in the obtaining of **private information** about a person (whether or not that person is the target of the investigation or operation); and

mmmmm) in a planned manner and not by way of an **immediate response** whereby it would not be reasonably practicable to obtain an authorisation prior to the surveillance being carried out.

Private Information includes any information relating to a person's private or family life including activities of a professional or business nature.

Intrusive Surveillance

A local authority **cannot** authorise **intrusive surveillance**.

Intrusive surveillance is defined as 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 any individual other than a CHIS on the premises or in the vehicle or is carried out by means of a **surveillance device**.

If the device is not located on the premises or in the vehicle, it is not intrusive surveillance unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

3. WHAT IS A COVERT HUMAN INTELLIGENCE SOURCE?

RIPA defines a CHIS as a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that

- covertly uses such a relationship to obtain information or to 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.

A relationship is covert if it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

THE USE OF A CHIS WILL ONLY BE AUTHORISED IN EXCEPTIONAL CIRCUMSTANCES.

The Council would have an ongoing duty of care to a CHIS and their safety and welfare would be paramount. Other methods of obtaining the information should be used if at all possible. Legal Services should be contacted at the outset as the rules and procedures are complicated.

There are additional safeguards in place which apply to the use of persons under the age of 18 as CHIS and also to vulnerable individuals. A vulnerable individual is a person who is or maybe in need of community care services by reason of mental or other disability, age or illness and who is unable to take care of themselves or unable to protect themselves from harm or exploitation.

A named officer (**a handler**) would have day to day responsibility for dealing with a CHIS and a further named senior officer would have oversight of the use made of the CHIS (**a controller**). A further officer (**a record keeper**) would be responsible for maintaining records relating to the CHIS and use of the CHIS. A risk assessment would be carried out prior to the use of the CHIS to determine the risk to them and the likely consequences should their role become known. This would be reviewed regularly during the course of the investigation and all necessary steps taken to ensure the safety and welfare of the CHIS during the course of the investigation and once the authorisation had been cancelled. It would be necessary to maintain a record of the use made by the CHIS, and regulate access to them, ensuring that the Regulation of Investigatory Powers (Source Records) Regulations 2006 are fully complied with.

4. COMMUNICATIONS DATA

Local authorities are only permitted to acquire communications data for the purpose of preventing or detecting serious crime. This is an offence punishable by a maximum term of 12 months imprisonment or more.
The request must be made through a qualified single point of contact accessed via the National Anti-Fraud Network and must also receive prior judicial approval.

Use of the Internet and Social Networking Sites

Use of the internet to gather information in the course of an investigation may amount to directed surveillance and officers should consider the intended purpose and the scope of the online activity it is proposed to take. The following factors should be taken into account:

- Whether the investigation or research is directed towards an individual.
- Whether it is likely to result in obtaining private information about a person or group of people.
- Whether it is likely to involve visiting internet sites to build up a profile.
- Whether the information obtained will be recorded and retained.
- Whether the information is likely to provide a pattern of lifestyle.
- Whether the information is being combined with other sources of information, which amounts to information relating to a person's private life.
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s).

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.
- Conversely, where the Council has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt, and a directed surveillance authorisation will not normally be available.

Normal usage

Where an investigator makes normal background checks on the internet, accessing pages that are in the public domain on a single occasion, this would be considered normal usage. Under these circumstances, whilst full records must be kept (in order to comply with the Criminal Procedure and Investigations Act) there is no need for investigators to seek RIPA authorisation to make these enquiries. During the course of the investigation, it would be normal for an investigator to make very occasional checks on pages, in order to confirm the information contained therein or, for example, to check for changes just prior to interview. If, following on from this, investigators then wish to monitor pages, or extract information from them in order to keep check on a suspect's activities, this may amount to Directed Surveillance.

Directed Surveillance

Where investigators make regular checks of social media, in order to monitor activity, this may amount to Directed Surveillance. This is because the person, whilst posting to a public forum, site or page, may well not expect the Local Authority to be watching them. As such, regardless of whether or not the user has sought to protect information by activating privacy settings, there will still be privacy implications.

An analogy must be drawn between the electronic world and the 'real' world - if investigators were to go to a public house, in order to listen to a conversation that the suspect was having, this would amount to Directed Surveillance; visiting an online forum for the same purpose is no different.

You wish to covertly watch a shop, in order to see if the shopkeeper is selling unlawful items. This is Directed Surveillance. That same shopkeeper has an online shop that you wish to check every day. What is the difference?

Covert Human Intelligence Source

Looking at publicity available pages is normally considered 'Open Source' investigation but the situation changes if investigators are required to request access, in order to view the page. If investigators have to create or maintain a 'personal or other relationship' in order to access information, this probably amounts to becoming a Covert Human Intelligence Source. A good example of this is 'Facebook', where a profile may be available for all to view ('Open Source' or Directed Surveillance) or may require investigators to send a friend request and have that request accepted. An Officer must not set up a false identity for a covert purpose without authorisation. An officer should not adopt the identity of a person known, or likely to be known, to the subject of interests or users of the site without authorisation, and without the explicit consent of the person whose identity is used, and without considering the protection of that person.

An exception would be where, for example, the officer uses an identity that is manifestly overt (NBBC Environmental Health Officer) and sends the request from this identity. Under these circumstances, the viewing of the page would amount to monitoring and not Directed Surveillance or becoming Covert Human Intelligence Source.

The Council's Internet and Social Media Investigation Procedure (February 2022) provides further information on the use of the internet and social media in the course of investigations and sets out a process to be followed by officers in situations where authorisation under RIPA is not required (non RIPA activity). Officers carrying out investigations must familiarise themselves with the Council's Policy on Covert Surveillance and the Internet and Social Media Investigation Procedure.

CCTV

The overt use of CCTV cameras in town centres, car parks etc is generally not regulated through RIPA. The Council's CCTV Policy and guidance from the Information Commissioner's Office provides more detail on the use of CCTV. However there may be instances where a law enforcement agency typically the Police, may wish to use the Council's CCTV system for Directed Surveillance. A written protocol exists between the Police and the Council which provides that CCTV operatives must be provided with a copy of the RIPA authorisation obtained by the Police prior to using the CCTV system for Directed Surveillance.

ANPR

The overt use of ANPR to monitor flow or detect offences does not require authorisation. However, if used in covert or pre planned operations or as part of a specific investigation of a person or group, a directed surveillance authorisation must be considered. Even where RIPA does not apply, CCTV systems are governed by data protection and human rights rules and regard must be had to the threshold in the Protection of Freedoms Act 2012.

5. THE ROLE OF DESIGNATED OFFICERS

Designated RIPA Co-ordinator, Senior Responsible Officer and Authorised Officers

RIPA Co-ordinator and Senior Responsible Officer

The following posts have been nominated as the designated RIPA Co-ordinator and Senior Responsible Officer for NBBC under the Regulation of Investigatory Powers Act 2000.

Officer:	Section:	Contact Details:
RIPA Co-ordinator ~~Wendy Davies-White~~Solicitor	~~Planning and~~ Corporate Resources~~Regulation~~	~~Tel: 024 7637 6100~~ ~~mailto: wendy.davies-white@nuneatonandbedworth.gov.uk~~ legal@nuneatonandbedworth.gov.uk
Deputy RIPA Co-ordinator ~~Shehnaz Tai~~Solicitor	Corporate Resources ~~Planning and Regulation~~	legal@nuneatonandbedworth.gov.uk ~~Tel: 024 7637 6268~~ ~~mailto: shehnaz.tai@nuneatonandbedworth.gov.uk~~
Senior Responsible Officer ~~Philip Richardson~~ Assistant Director – Governance & Democracy	Corporate Resources ~~Planning and Regulation~~	Tel: 024 7637 ~~6233~~6250 ~~mailto:~~ ~~philip.richardson~~matthew.wallbank@nuneatonandbedworth.gov.uk legal@nuneatonandbedworth.gov.uk
Deputy Senior Responsible Officer Solicitor to the Council ~~Waheeda Sheikh~~	Corporate Resources ~~Planning and Regulation~~	Tel: 024 7637 6897 ~~mailto:~~ waheeda.sheikh@nuneatonandbedworth.gov.uk legal@nuneatonandbedworth.gov.uk

Authorising Officers

The following Officers shall be designated as Authorising Officers for the specified purpose on behalf of NBBC under the Regulation of Investigatory Powers Act 2000.

Power to authorise delegated to post-holder:	DCS	Confidential Material:
Chief Executive	Yes	Yes

Formatted Table

Commented [MW1]: Details to be confirmed subject to recruitment

Formatted: Font: (Default) Arial, 12 pt, Underline

Field Code Changed

Commented [MW2]: Details to be confirmed subject to recruitment

Formatted: Font: (Default) Arial, 12 pt, No underline

Formatted: Space After: 0 pt, Line spacing: single

Field Code Changed

Formatted: Justified, Space After: 0 pt, Line spacing: single, Tab stops: 3.56 cm, Centered

Field Code Changed

Formatted Table

~~Director – Customer and Corporate Services & Deputy Chief Executive~~Strategic Director – Corporate Resources	Yes	~~Yes (in the absence of the Chief Executive)~~ TBC
Strategic Director – ~~Regeneration and~~ Housing and Community Safety~~,~~	Yes	~~No~~ TBC
Strategic Director – Public Services	Yes	TBC~~No~~
Strategic Director – Place and Economy	Yes	TBC

Commented [MW3]: TBC - subject to Deputy Chief Executive appointment

Formatted: Justified, Space After: 0 pt, Line spacing: single

Formatted: Font: (Default) Arial, 12 pt

NB: There is no provision for other officers to authorise investigations even in cases of emergency. Only the Chief Executive or in his absence the Deputy Chief Executive can authorise investigations that will involve the collection of confidential material.

Elected Members

Regular reports on the number and type of authorisations granted will be taken to Overview and Scrutiny Panel.

Role of the Senior Responsible Officer

The Senior Responsible Officer is responsible for:

- ensuring processes are in place within the Council to authorise surveillance in compliance with the RIPA legislation and Codes of Practice
- engagement with the Commissioner and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner
- ensuring that all relevant officers receive regular training
- error reporting to IPCO within 10 working days for example surveillance without lawful authority or failure to comply with law or codes of practice

6. AUTHORISATION PROCESS

An authorisation under Part II of the Act will provide lawful authority for a public authority to carry out surveillance.

An application for authorisation must be made on the prescribed form which is available at RIPA forms - GOV.UK (www.gov.uk). A separate risk assessment should also be undertaken and provided to the Authorising Officer.

The flowcharts in Annex 1 shows the steps which are required in the authorisation procedure.

Employees are advised to discuss the need to undertake DCS with their line manager and Legal Services before seeking authorisation. The line manager must endorse the application form before submitting it to the Authorising Officer. Options to gain the information, which is required, other than by using covert techniques, should be fully explored.

An applicant should complete the application form addressing the following points:

- The action to be authorised.
- The identities, where known, of those to be the subject of directed surveillance.
- An account of the investigation or operation.
- An explanation of the covert techniques that will be used
- Confirmation that the action proposed is intended to prevent or detect crime
- A statement outlining why the surveillance technique is considered to be proportionate to what it seeks to achieve.
- Details of what a CHIS would be tasked with
- An explanation of the information which it is desired to obtain as a result of the authorisation.
- An assessment of the potential for collateral intrusion, that is to say, interference with the privacy of persons other than the subjects of the surveillance, and an assessment of the risk of such intrusion or interference.
- An assessment of the likelihood of acquiring any confidential material and how that will be treated.
- A risk assessment for use of a CHIS

The applicant should discuss the content of the form with the Authorising Officer

Authorisation must be given in writing by the Authorising Officer. To consent to an authorisation, the Authorising Officer must be satisfied that the proposed surveillance is **necessary** for the purpose of preventing and detecting crime that meets the crime threshold.

The Authorising Officer must also believe that the proposed surveillance is **proportionate** to what it seeks to achieve and that any potential for **collateral intrusion** and the likelihood of acquiring any **confidential material** is reduced to a minimum. Reference must be made to the statutory code of practice on covert surveillance.

Necessity

The Act requires the Authorising Officer to believe that the authorisation is necessary for the following reason.

> **For the purpose of preventing or detecting conduct which constitutes one or more criminal offences where the offence is punishable whether on Summary Conviction or**

Indictment by a maximum term of at least 6 months imprisonment or certain prescribed licensing offences e.g. sales to minors

Proportionality

The Authorising Officer must also be satisfied that the proposed surveillance is proportionate to what it seeks to achieve. This should include an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the provincial "sledgehammer to crack a nut"). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. Authorising Officers must balance the human rights of the individual against the need to undertake covert surveillance to further an investigation. It is insufficient to simply say that the 'seriousness' of the crime justifies the potential method. Similarly any potential cost savings cannot be used to justify use of technological solutions which are often capable of being more intrusive than a human being.

These 4 elements of proportionality must be fully considered.

i) balancing the size and scope of the operation against the gravity and extent of the perceived mischief
ii) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
iii) that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result and
iv) evidencing what other methods have been considered and why they were not implemented.

The Authorising Officer should set out why he/she believes that the proposed action is necessary and proportional. A bare assertion is insufficient. Authorising officers must state explicitly what is being authorised

Collateral Intrusion

Before authorising surveillance the Authorising Officer must also take into account the risk of intrusion into the privacy of persons other than those who are the subject of the investigation. Measures should be taken to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation. Authorising Officers need to fully understand the capabilities and sensitivity levels of any technical equipment intended to be used and where and how it is to be deployed. An application for an authorisation should include an assessment of the risk of any collateral intrusion. The Authorising Officer should take this into account, when considering the proportionality of the surveillance. To assist in this process a map of the area should be attached to the application indicating particularly sensitive items such as schools.

Confidential Material

is anything:

- That is subject to legal privilege, for example communications between a legal adviser and his/her client.
- That is confidential personal information, for example information about a person's health or spiritual counselling or other assistance given or to be given to him or her.
- That is confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and subject to an undertaking to hold in confidence

The Authorising Officer will consider the content of the application form and address the issues of necessity and proportionality and make a decision as to whether to approve or refuse the application

The Authorising Officer will specify dates when the authorisation should be reviewed and the frequency of review thereafter but these should be completed at least monthly. A review form has to be completed to record any review that does take place.

Approval of Local Authority Authorisation by a Justice of the Peace

The flowcharts at Annex 1 outline the procedure for applying for judicial approval. The application must be made by the public authority that has granted the authorisation. Following approval by the authorising officer, the RIPA Coordinator will contact the magistrates' court to arrange a hearing.

The local authority will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. In addition, the local authority will provide the JP with a partially completed judicial application/order form.

The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.

The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters and as such the case investigator must attend the hearing. It is good practice for the authorising officer also to attend to assist the Magistrate if required. It is not envisaged that the skills of legally trained personnel will be required to make the case to the JP and this would be likely to, unnecessarily, increase the costs of local authority applications.

Following their consideration of the case the JP will complete the order section of the judicial application/order form recording their decision.

The JP may decide to

Approve the Grant or renewal of an authorisation or notice

The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation or notice

The RIPA authorisation or notice will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.

The court must not exercise its power to quash that authorisation or notice unless the application has had at least 2 business days from the date of the refusal in which to make representations.

A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the local authority should consult their legal advisers.

Duration of Authorisation

A written authorisation granted by an authorising officer and approved by a Magistrate will take effect when signed by the Magistrate. It will automatically cease to have effect unless renewed or cancelled at the end of a period of three (3) months beginning with the day on which it took effect. CHIS authorisations last for 12 months (1 month if the CHIS is 18).

Record of Authorisations

All completed application forms, renewal forms and cancellation forms must be immediately sent to the RIPA Co-ordinator. Copies should be kept by the Authorising Officer and by the Applicant for retention on the investigation file.

In all cases, the relevant section must retain the following documentation which does not form part of the centrally retrievable record held by the RIPA Co-ordinator

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- copy of the Justice of the Peace Approval
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the authorising officer

In respect of a CHIS full details of the CHIS and the management arrangements must be kept by the Record Keeper including:

- The identity of the CHIS
- The identity or identities used by the CHIS, where known
- The means used within the Council of referring to the CHIS
- Any significant information connected with the security and welfare of the CHIS
- Any confirmation made by an Authorising Officer granting or renewing an authorisation for the conduct or use of a source, that the security and welfare of the CHIS has been considered and that any identified risks to the security and welfare of the CHIS have been properly explained to and understood by the CHIS
- The date when, and the circumstances in which, the CHIS was recruited
- The authority for the related investigation or operation
- The identities of the Controller, the Handler, and the Record Keeper
- The period for which those responsibilities have been discharged by those persons
- The tasks that are given to the CHIS and the demands made of him in relation to his activities as a CHIS
- All contacts or communications between the CHIS and the Council or where the CHIS is a Council Officer, the Handler, and the Controller.
- The information obtained by the Council by the conduct or use of the CHIS

- In the case of a CHIS who is not an Officer of the Council, every payment, benefit or reward or every offer of a payment, benefit or reward that is made or provided by or on behalf of the Council in respect of the CHIS's activities for the benefit of the Council

Central Record of Authorisations

A centrally retrievable record of all authorisations is held by the RIPA Co-ordinator which is up-dated whenever an authorisation is granted, renewed or cancelled. These records are retained for a period of at least **three years** from the ending of the authorisation and contain the following information:

- The type of authorisation;
- The date the authorisation was given;
- The name and title of the Authorising Officer;
- The unique reference number of the investigation;
- The title of the investigation, including a brief description and the names of the subjects, if known;
- Whether the urgency provisions were used and why;
- If the authorisation is renewed, when it was renewed and the name and title of the Authorising Officer;
- Whether the investigation is likely to result in obtaining confidential information; and
- The date the authorisation was cancelled.

Additional records must be maintained by a CHIS Record Keeper which include full details of the CHIS and the management arrangements.

7. AFTER APPROVAL OF AUTHORISATIONS

After authorisation the Authorising Officer must continue to oversee the progress of the investigation. He or she must ensure that whatever was authorised does actually happen and that actions do not exceed the boundaries of the authorisation. Progress should be reviewed in accordance with the authorisation. In any case, as soon as the objectives have been achieved a **cancellation must be issued**.

It will be the responsibility of the officer in charge of an investigation to ensure that any surveillance activity is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. The RIPA Co-ordinator shall also perform a monitoring role in this respect **but the primary responsibility rests with the Authorising Officer.**

Reviews

Regular reviews (at least monthly) of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable. Reviews do not need to go before a JP.

Renewals

An Authorising Officer and Justice of the Peace may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was

given. Such renewals would normally extend the authorisation period for a further three months beginning with the day on which initial authorisation would cease to have effect, but for the renewal. Authorisation may be granted more than once, provided they continue to meet the criteria for authorisation. An application for renewal must not be made more than **seven days** before the authorisation is due to expire and must consider the same criteria as a new application

Cancellations

All authorisations, including renewals, **must** be cancelled if the reason why DCS was required no longer exists. This will occur in most instances when the purpose for which surveillance was required has been achieved and officers must be mindful of the need to cancel any authorisation which has been issued. A cancellation should be issued at the expiry date if not before. The responsibility to ensure that authorisations are cancelled rests with the Authorising Officer.
Cancellations do not need to go before a JP.

All completed cancellation forms must be sent to the RIPA Co-ordinator. A copy of the form should be retained by the Authorising Officer and a further copy sent to the Applicant for retention on the investigation file.

8. RETENTION AND DESTRUCTION OF DOCUMENTS

All applications for authorisation (including those that have been refused), renewals and cancellations will be retained for a period of at least **five years** by the RIPA Co-ordinator. They will then be considered for destruction.

The Central Register will be kept for at least **three years**. Individual records will be considered for destruction after that time.

Individual sections should retain their documentation and a record of all applications and authorisations for a period of **five years** from the ending of the authorisation.

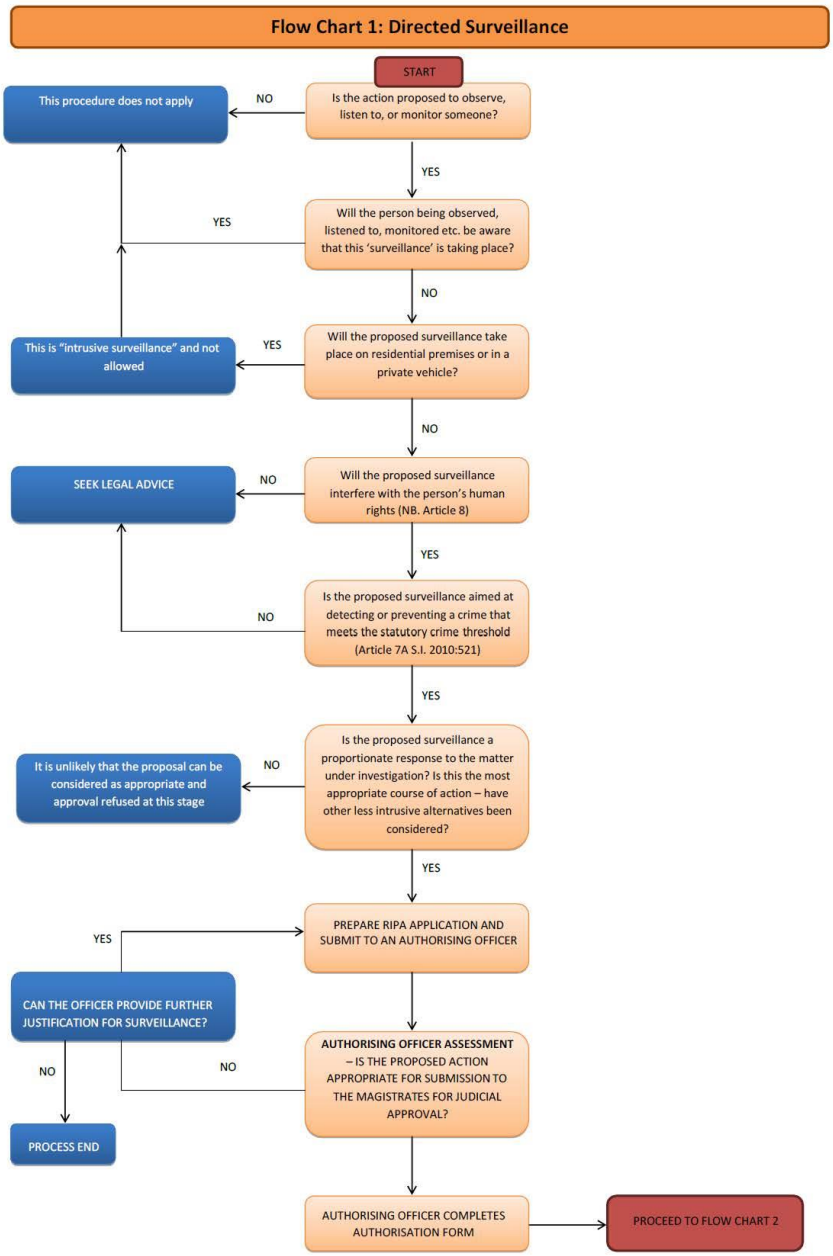
Regard should be had to the Council's Document Retention Policy.

Annex 1 Flow charts[1]

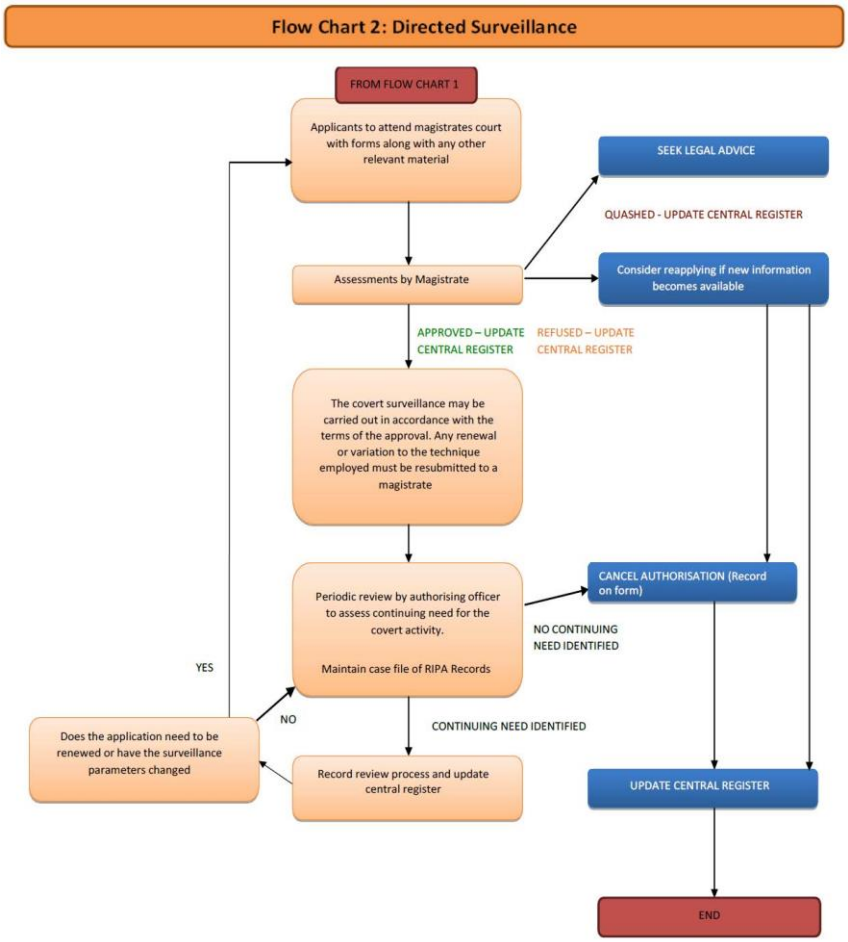
Flow chart 1 Directed Surveillance
Flow chart 2 Directed Surveillance - Authorisation by Justice of the Peace
Flow chart 1 Use and Authorisation of CHIS
Flow chart 2 Use and Authorisation of CHIS - Authorisation by Justice of the Peace

[1] Flowcharts reproduced with kind permission from Cardiff Council

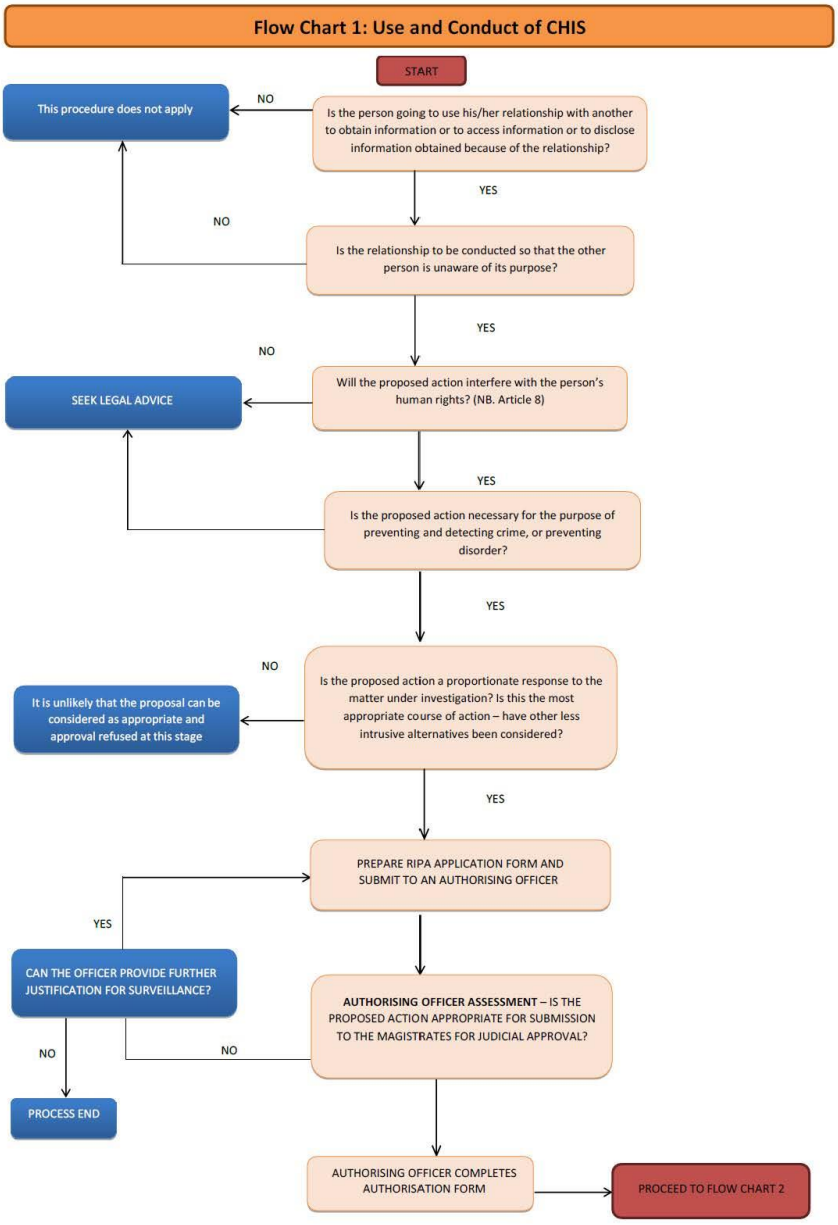
Appendix A


Flow Chart 1: Directed Surveillance
START
Is the action proposed to observe, listen to, or monitor someone?
NO
This procedure does not apply
YES
Will the person being observed, listened to, monitored etc. be aware that this 'surveillance' is taking place?
YES
NO
Will the proposed surveillance take place on residential premises or in a private vehicle?
YES
This is "intrusive surveillance" and not allowed
NO
Will the proposed surveillance interfere with the person's human rights (NB. Article 8)
NO
SEEK LEGAL ADVICE
YES
Is the proposed surveillance aimed at detecting or preventing a crime that meets the statutory crime threshold (Article 7A S.I. 2010:521)
NO
YES
Is the proposed surveillance a proportionate response to the matter under investigation? Is this the most appropriate course of action – have other less intrusive alternatives been considered?
NO
It is unlikely that the proposal can be considered as appropriate and approval refused at this stage
YES
PREPARE RIPA APPLICATION AND SUBMIT TO AN AUTHORISING OFFICER
YES
CAN THE OFFICER PROVIDE FURTHER JUSTIFICATION FOR SURVEILLANCE?
NO
NO
PROCESS END
AUTHORISING OFFICER ASSESSMENT – IS THE PROPOSED ACTION APPROPRIATE FOR SUBMISSION TO THE MAGISTRATES FOR JUDICIAL APPROVAL?
AUTHORISING OFFICER COMPLETES AUTHORISATION FORM
PROCEED TO FLOW CHART 2

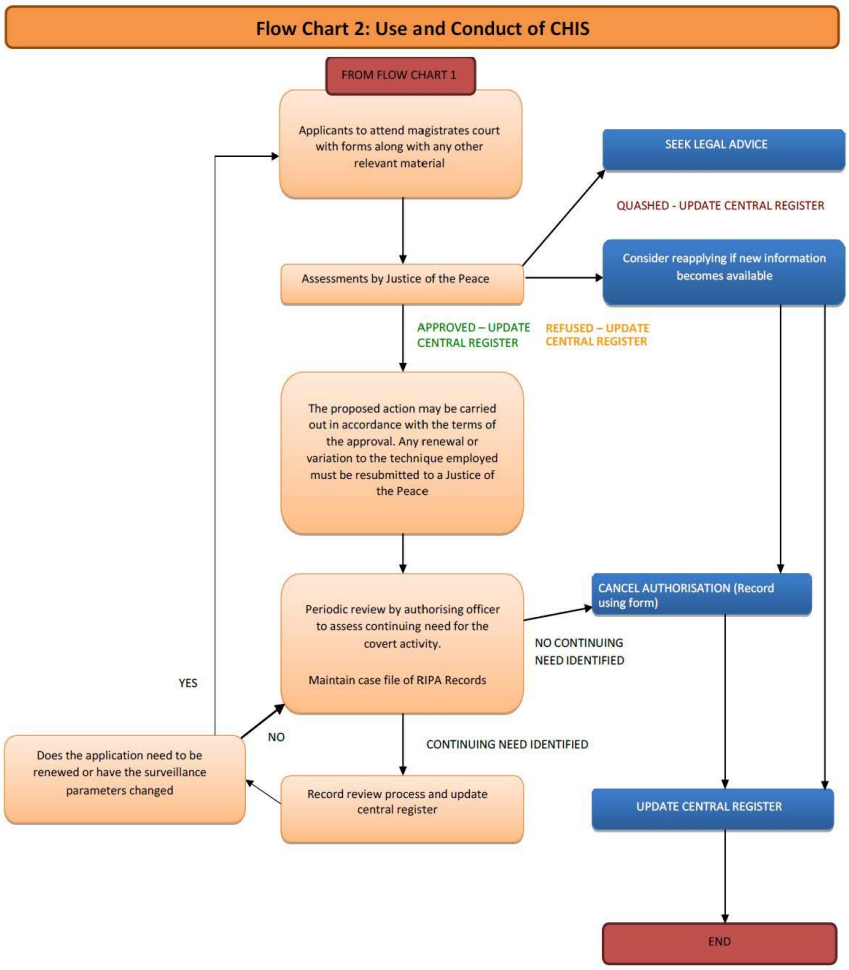
Appendix A


Flow Chart 2: Directed Surveillance
FROM FLOW CHART 1
Applicants to attend magistrates court with forms along with any other relevant material
SEEK LEGAL ADVICE
QUASHED - UPDATE CENTRAL REGISTER
Assessments by Magistrate
Consider reapplying if new information becomes available
APPROVED – UPDATE CENTRAL REGISTER
REFUSED – UPDATE CENTRAL REGISTER
The covert surveillance may be carried out in accordance with the terms of the approval. Any renewal or variation to the technique employed must be resubmitted to a magistrate
Periodic review by authorising officer to assess continuing need for the covert activity.
Maintain case file of RIPA Records
CANCEL AUTHORISATION (Record on form)
NO CONTINUING NEED IDENTIFIED
YES
NO
CONTINUING NEED IDENTIFIED
Does the application need to be renewed or have the surveillance parameters changed
Record review process and update central register
UPDATE CENTRAL REGISTER
END

Appendix A


Flow Chart 1: Use and Conduct of CHIS
START
Is the person going to use his/her relationship with another to obtain information or to access information or to disclose information obtained because of the relationship?
NO
This procedure does not apply
YES
Is the relationship to be conducted so that the other person is unaware of its purpose?
NO
YES
Will the proposed action interfere with the person's human rights? (NB. Article 8)
NO
SEEK LEGAL ADVICE
YES
Is the proposed action necessary for the purpose of preventing and detecting crime, or preventing disorder?
YES
Is the proposed action a proportionate response to the matter under investigation? Is this the most appropriate course of action – have other less intrusive alternatives been considered?
NO
It is unlikely that the proposal can be considered as appropriate and approval refused at this stage
YES
PREPARE RIPA APPLICATION FORM AND SUBMIT TO AN AUTHORISING OFFICER
YES
CAN THE OFFICER PROVIDE FURTHER JUSTIFICATION FOR SURVEILLANCE?
AUTHORISING OFFICER ASSESSMENT – IS THE PROPOSED ACTION APPROPRIATE FOR SUBMISSION TO THE MAGISTRATES FOR JUDICIAL APPROVAL?
NO
NO
PROCESS END
AUTHORISING OFFICER COMPLETES AUTHORISATION FORM
PROCEED TO FLOW CHART 2

Appendix A


Flow Chart 2: Use and Conduct of CHIS
FROM FLOW CHART 1
Applicants to attend magistrates court with forms along with any other relevant material
SEEK LEGAL ADVICE
QUASHED - UPDATE CENTRAL REGISTER
Assessments by Justice of the Peace
Consider reapplying if new information becomes available
APPROVED – UPDATE CENTRAL REGISTER
REFUSED – UPDATE CENTRAL REGISTER
The proposed action may be carried out in accordance with the terms of the approval. Any renewal or variation to the technique employed must be resubmitted to a Justice of the Peace
Periodic review by authorising officer to assess continuing need for the covert activity.
Maintain case file of RIPA Records
CANCEL AUTHORISATION (Record using form)
NO CONTINUING NEED IDENTIFIED
YES
NO
CONTINUING NEED IDENTIFIED
Does the application need to be renewed or have the surveillance parameters changed
Record review process and update central register
UPDATE CENTRAL REGISTER
END

This document is also available in other languages on request:

এই ডকুমেন্ট অন্য ভাষায়, বড় প্রিন্ট আকারে এবং অডিও টেপ আকারেও অনুরোধে পাওয়া যায়।

આ દસ્તાવેજ વિનંતી કરવાથી બીજી ભાષાઓ, મોટા છાપેલા અક્ષરો અથવા ઓડિઓ રચનામાં પણ મળી રહેશે.

अनुरोध पर यह दस्तावेज़ अन्य भाषाओं में, बड़े अक्षरों की छपाई और सुनने वाले माध्यम पर भी उपलब्ध है

本文件也可应要求，制作成其它语文或特大字体版本，也可制作成录音带。

Dokument ten jest na życzenie udostępniany także w innych wersjach językowych, w dużym druku lub w formacie audio.

ਇਹ ਦਸਤਾਵੇਜ਼ ਹੋਰ ਭਾਸ਼ਾਵਾਂ ਵਿਚ, ਵੱਡੇ ਅੱਖਰਾਂ ਵਿਚ ਅਤੇ ਆਡੀਓ ਟੇਪ 'ਤੇ ਰਿਕਰਾਡ ਹੋਇਆ ਵੀ ਮੰਗ ਕੇ ਲਿਆ ਜਾ ਸਕਦਾ ਹੈ।

درخواست پر یہ دستاویز دیگر زبانوں میں، بڑے حروف کی چھپائی اور سننے والے ذرائع پر بھی میسر ہے۔

Also available in Large Print, CD Rom, Audio Tape and Braille on request.
Contact us on: **02476 376 328**

typetalk: **18001 024 7637 6328**

Language Line services

Nuneaton & Bedworth

United to Achieve

Policy in Relation to Monitoring and Surveillance in the Workplace

Issued by Human Resources

NUNEATON & BEDWORTH BOROUGH COUNCIL

Policy in Relation to Monitoring and Surveillance in the Workplace

Quality Record

Issue No.	Date	Initial EIA	Stage	Agreed
1	April 2024		Draft	
2	June 2024		Union Consultation	
3	July 2024	Y	EIA	RB

This document is available in larger print.

Please contact Human Resources for a larger copy

NUNEATON & BEDWORTH BOROUGH COUNCIL

Policy in Relaiton to Monitoring and Surveillance in the Workplace

Contents

1. Introduction

Nuneaton and Bedworth Borough Council is committed to developing a workplace culture where there is a respect for the private life, data protection, security and confidentiality of personal information, and the Council complies with the requirements of data protection legislation and Information Commissioner's Office (ICO) Employment Practices Code.

The Council is committed to treating all staff members fairly and this policy aims to provide consistency in the treatment of all staff. Serious infringement of data protection rules including in relation to the collection, content inspection, use and storage of data through the monitoring and surveillance systems in the workplace, will be treated as a serious disciplinary matter.

This policy should be read in conjunction with a number of other policies, noted in more detail in section 3.

There may be other circumstances that arise that are not covered by this policy. Individual circumstances cannot always be accounted for within a written procedure and where circumstances arise that are not covered by this document, these should be discussed with an HR.

2. Purpose

The Council recognises that there is a need to balance staff privacy in the workplace along with ensuring the health and safety of staff and that the Council is complying with regulatory and statutory obligations.

This policy aims to provide this balance in the monitoring and surveillance undertaken in the workplace and how such information may be utilised.

3. Scope

This Policy and any associated procedures will apply to all Council employees including those employees working on a temporary or fixed term contract. It also applies to casual, agency and contract workers and elected members.

4. Responsibilities

Failure to adhere to the processes within the Procedure may lead to disciplinary action.

4.1 Managers

Managers should ensure that all staff members are aware of this policy and understand their own and the employer's responsibilities. Training on data protection and privacy issues will be provided to all managers. Employees

should be reminded at regular intervals of this policy and related policies and where to find them.

Where managers may have access to and make use of surveillance tools in the course of their work, they have a responsibility to ensure that such monitoring is relevant and information is used appropriately in line with legislation.

4.2 Employees

All employees will be required to undertake an appropriate level of training relevant to their role in relation to data protection and privacy issues.

Employees also need to be aware of and comply with relevant associated policies, with particular reference to use of work resources for personal use.

4.3 Human Resources

Human Resources are responsible for providing timely and up to date professional advice, guidance on process and support to managers and employees to assist with the effective management of this Policy.

4.4 Data Protection Officer

The Council's appointed officer responsible for Data Protection will ensure that this policy is applied consistently and that any issues that arise in relation to privacy are dealt with appropriately.

4.5 Trade Unions

Trade Unions will work with managers, employees and Human Resources to ensure the policy is applied fairly and consistently across the Council.

5. Relevant Legislation

There is a number of specific legalisation that will impact and inform the monitoring and surveillance noted under this policy.

5.1 The Human Rights Act The Human Rights Act 1998

This Act sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights . In particular, Article 8 provides individuals with the right to respect for private and family life, home and correspondence, subject to being "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country… or for the protection of the rights and freedoms of others." This right includes an individual's personal privacy within the workplace balanced against the legitimate business interests.

5.2 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018

This legislation is enforced by the Information Commissioner's Office (ICO) and regulates the use and processing of personal data. More information can be found in the Council's Data Protection Policy but in summary and in relation to monitoring and surveillance in the workplace specifically, the following are examples of relevant personal information may be gathered for employees:

- Pay roll number
- Date of birth
- National insurance number
- Bank details
- Email address
- Telephone number
- Home address
- Photographs
- Telephone recordings
- CCTV recordings
- Equality and Diversity information

5.3 Protection of Freedoms Act 2012

This Act includes a statutory code of practice on the use of surveillance cameras and a surveillance camera commissioner was appointed with responsibility for reviewing and reporting on the operation of the code. Therefore, it is of relevance in relation to CCTV surveillance in workplaces.

5.4 The Regulation of Investigatory Powers Act (RIPA) 2000

Depending upon the circumstances, the RIPA allows security services and in some cases the public bodies mentioned in the legislation the right to use digital surveillance and access digital communication held by a person or organisation. This may apply to some situations where there is surveillance of an employee carried out as part of a disciplinary investigation by the Council as a public authority.

6. Associated Policies

The Council has several policies and procedures that should be read in conjunction with this policy. These include but are not limited to:

- ICT code of Conduct
- Social Media Policy
- Asset Management Policy (Vehicle Tracking)
- RIPA Policy
- CCTV and Security Policy

In addition, other information may be gathered in relation to employees to better aid business decisions. This may include information collected as part of pre-employment, health information and other HR metric data that may be used to inform workforce development and other strategies.

6.1 ICT and Telephony – Appropriate Use

The Council has a ICT code of Conduct policy that provides a framework for acceptable use of IT, emails and phones issued for work purposes.

Under the Policy the Council has the right to specify which websites can or cannot be visited by employees. This will include the use of website blocking software, to prevent employees from accessing certain websites. The Council will take steps to monitor and retain data on access to websites.

The Policy also covers e-mail usage that limits personal use. It should be noted that employees have no legal right to use their employer's email, internet or make phone calls for personal use. However, the Council allows for limited and reasonable use of work IT, email and phones for personal use.

Employees should note that the Council has a right to access employees' emails and voicemail while they are away from work to deal with matters of business, so long as employees have been informed that this is going to happen.

6.2 CCTV (and/or other tracking or audio recording arrangements)

CCTV is used within most of the Council's Corporate buildings. It will also be used in other public areas across the Borough. In the main, CCTV within corporate buildings is used to ensure the safety of employees and of customers or service-users. This may also include body worn cameras which may be used by certain roles.

Such recording devices may pick up audio recordings as well as images. The main aim of using such devices is to protect the safety of people (e.g. as part of a preventative measure for lone workers). They are also used to enhance the security and safety of premises and property.

Where CCTV is in use in the workplace, such areas will be clearly signposted It should also be made clear to them who is able to watch footage and when it will be watched. Further information on the use of, access to and release of CCTV footage is available in the Council's CCTV and Surveillance Policy.

6.3 ID Passes and Door Security

The Council will issue a work ID badge to all employees. These badges include software that allows and limits access to corporate buildings. In the main, such data will be used for security reasons.

6.4 Vehicle Tracking Systems

The Council has an Asset Management Policy and a Drivers and Driving which details use of both vehicle tracking systems and Tachographs in more detail.

Tracking devices will be used in most Council fleet vehicles so that the location of vehicles, the distances the vehicle has travelled and any other information about the driver's driving habits can be tracked. This enables better allocation of duties and tasks as well as ensuring the safety and welfare of our employees.

Tachographs are a legal requirement and are used to monitor the driving duration of those drivers who fall within the regulations.

7. Covert Monitoring

Covert monitoring by definition includes the recording of employees without their knowledge. Covert monitoring will not be used by the Council in the workplace.

There may be times where during the course of work, managers may undertake on the spot checks, such as unannounced site inspections. This may be for routine audits or following complaints or concerns raised by members of the public, for example about work practises. Where such visits result in potential issues of misconduct, appropriate witness statements will be taken.

8. Use of monitoring and surveillance information in a disciplinary and/or grievance cases

The Council reserves the right to use work emails, CCTV and other surveillance data as part of evidence for formal disciplinary and/or grievance investigations.

Where such evidence is used, the investigation should ensure where possible that this can be corroborated as far as possible by other information, such as witness statements.

Where CCTV and other surveillance evidence is used, such information must be used objectively and in full (particularly evidence based on CCTV footage). Copies of such evidence should be made available to those employees subject to such investigations.

9. Releasing information to prevent or detect crime

The police or other crime prevention / law enforcement agencies (e.g. Benefit Fraud Office and local authority functions) may at time contact the Council and request that personal data is disclosed in order to help them prevent or detect a crime. This will include any information collected in relation to employees under this policy.

Although the Council is not legally obliged to comply with such requests, the data protection regulation does allow organisations to release the information if they decide it is appropriate.

Before any decision is made about disclosure, the Council will consider the following:

- The impact on the privacy of the individual/s concerned • Any duty of confidentiality owed to the individual/s
- Whether refusing disclosure would impact the requesting organisation's ability to detect, prevent or prosecute an offender.

In most cases, the Council will comply with such requests and release appropriate information. However, if a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for the employer to release the information.