North Northamptonshire Council

POLICY ON THE USE OF INVESTIGATORY POWERS UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) AND THE INVESTIGATORY POWERS ACT 2016 (IPA)

June 2022

www.northnorthants.gov.uk

Document Version Control

Author (Post holder title): Director of Governance & HR
Type of document: Policy
Version Number: 1.0
Document File Name:
Issue date: May 2022
Approval date and by who (CMT / committee):
Document held by (name/section):
For internal publication only or external also?: Both
Document stored on Council website or Intranet?:
Next review date: June 2023

Change History

Issue	Date	Comments

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
Corporate Enforcement Group	

Distribution List

Internal	External
	e.g. Stakeholders / Partners /Organisation(s)

Links to other documents

Document	Link
Enforcement Policy	Enforcement policy | North Northamptonshire Council (northnorthants.gov.uk)

Contents

1.0 Introduction

1.1 This document sets out North Northamptonshire Council's ('NNC') policy on human rights, the requirements of the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the relevant Home Office Codes of Practice made thereunder including those on Covert Surveillance and Property Interference, Covert Human Intelligence Sources, the Investigation of Protected Electronic Information and Communications Data. It should be read in conjunction with the NNC guidance notes.

1.2 In carrying out the law enforcement functions of NNC, officers of the Council may need to use the above methods where it is necessary and proportionate to do so.

1.3 To ensure easy access, a copy of this document, the guidance and related forms will be accessible on the Council intranet.

2.0 Scope

2.1 The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) provide for, and regulate the use of, a range of investigative powers, by a variety of public authorities. RIPA and IPA are consistent with the Human Rights Act 1998 and create a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (ECHR) which states that any interference by a public authority with the right to respect for a person's private and family life, his home, or his correspondence, are carried out in accordance with law.

2.2 If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Investigatory Powers Tribunal, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and would undoubtedly, be the subject of adverse media coverage. It is essential, therefore, that all NNC Services comply with this Policy and any further guidance that may be issued, from time to time.

3.0 Policy

3.1 NNC is committed to the principles of equality and social justice in both employment and delivery of services.

3.2 Being a public authority, NNC recognises that it has:

a) a vital role to play in ensuring that the aims of the ECHR and the Human Rights Act 1998 are given practical effect.

b) a positive obligation to ensure that respect for human rights is at the core of its day-to-day work.

c) a responsibility to ensure that its decisions and procedures do not infringe human rights; and

d) a responsibility to ensure that any decisions which affect human rights are carefully reasoned and recorded.

3.3 NNC is committed to ensuring that:

a) any of its activities, including internet and social media investigations, which might interfere with the right to respect for a person's private and family life, his home, or his correspondence, are carried out lawfully and have regard to RIPA and IPA.

b) it keeps under review its activities to determine those which fall within the scope of RIPA and IPA.

c) it has policies, procedures, and documentation to ensure that relevant investigatory powers (i.e. relating to the obtaining of communications data, the use of covert surveillance in the course of specific operations and the use of covert human intelligence sources, such as agents, informants, and undercover officers) are used in accordance with human rights and the provisions of RIPA and IPA and Codes of Practice made thereunder.

d) all staff whose activities may involve the use of practices under RIPA are competent to conduct the duties required, have undertaken training in the implementation of the Service policy, the procedures and the documentation relating to this subject.

e) any officer, who is identified as an authorising or verifying officer for the purpose of RIPA or IPA, is at an appropriate level and is competent to conduct the duties required.

f) surveillance equipment is kept under central management and a central record of all authorisations is maintained and regularly updated whenever an authorisation is granted, renewed, or cancelled.

g) a Senior Responsible Officer is appointed to ensure the integrity of the processes that are in place in order to confirm compliance with RIPA and IPA and the Codes of practice.

h) this policy is reviewed on an annual basis by elected members.

i) a regular review of the use of RIPA by the Council is conducted to ensure that the powers are being used consistently in accordance with this policy and that the policy remains fit for purpose.

Designation of Authorising Officers

3.4 The following posts will be designated posts under RIPA or the IPA. These are the only posts that may authorise the use of Covert Surveillance, Covert Human Intelligence Sources or to verify the obtaining of Communications Data:

- Assistant Director of Regulatory Services in Place and Economy;
- Executive Director of Place and Economy;
- Executive Director of Adults Communities and Wellbeing;
- Chief Executive (Head of Paid Service);

3.5 These officers are of the appropriate seniority within the Council, as required by the legislation.

3.6 Authorising Officers, when making authorisations under RIPA, must be aware that each authorisation (or renewal of an authorisation), will be subject to judicial approval.

3.7 The list will be kept up to date by the Senior Responsible Officer (SRO) and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, they must refer such request to the SRO for consideration, as necessary. The SRO is duly authorised to add, delete or substitute a post.

3.8 When knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source, the authorisation level will be Head of Paid Service or (in their absence) the person acting as Head of Paid Service.

The Senior Responsible Officer and Responsibilities

3.9 The SRO shall be a member of the Corporate Management Team and be the Director of Governance and HR. The SRO will ensure the integrity of the processes in place in relation to the use of covert human intelligence sources, surveillance, and the obtaining of communications data within the Council and monitor compliance with the Act and any relevant codes of practice. They will also liaise with the relevant Inspectors when an inspection is undertaken and oversee the implementation of any post-inspection action plans.

3.10 The Investigatory Powers Commissioner (IPC) aims to inspect each council in England, Wales, and Scotland once every three years. Before compiling any documentation requested by the IPC, the SRO will seek written confirmation from each Director whether any of their staff have engaged in activities covered by RIPA. In the event that no activities are reported, then a nil return is still required to be returned to the SRO.

Acquisition and Disclosure of Communications Data

3.11 The Council subscribes to the National Anti-Fraud Network ("NAFN") which is a non-profit making national Local Government Organisation. Its staff are Local Authority employees who are fully accredited and trained to deal with the obtaining of intelligence.

3.12 Applicants within local authorities who wish to obtain communications data are required to consult a NAFN single point of contact (SPoC) throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner.

3.13 NAFN is the single point of contact for all the Council's RIPA access to communications data requests. This will continue as a Collaborative Agreement under IPA.

3.14 For communication data requests, senior internal approval is required before an application is sent for independent authorisation. The SRO shall be satisfied that the officers verifying the application are of an appropriate rank and must confirm to NAFN the identity of the nominations.

Training

3.15 Training on the legislative requirements, the Council's policy and procedural arrangements will be arranged for:

a) officers identified as being likely to carry out activities regulated under RIPA;

b) officers who may carry out activities regulated under RIPA;

c) applicants;

d) designated authorising officers;

e) Senior Responsible Officer;

f) Head of Paid Service;

g) Members undertaking oversight or scrutiny of the use of RIPA/IPA powers;

h) Such other individuals as the SRO shall deem appropriate.

3.16 Training for those applying for or determining applications will be provided or arranged by the SRO in consultation with the Assistant Director, Regulatory Services and the Corporate Enforcement Group. A central record of training undertaken will be retained.

Oversight and Review of the Policy and Internal Reports

3.17 This policywill be kept under annual review by the SRO and the Assistant Director, Regulatory Services, supported by their respective deputies.

3.18 Elected members will review the Council's use of RIPA and set policy at least once a year. A report will be presented to elected members by the SRO.

3.19 There will be regular audits of compliance, in consultation with Services that make use of Covert Surveillance, Covert Human Intelligence Sources and the Obtaining of Communications Data. The audit will, as far as possible, include an assessment of all equality issues in relation to the practical implementation of the policy.

3.20 The report will be shared with the SRO and the appropriate services.

3.21 The Central Register of all RIPA authorisations, reviews, renewals, cancellations, and rejections will be maintained by the Assistant Director, Legal and Democratic Services ("the Record Keeping Officer").

4.0 Glossary of terms

Term	Definition
Authorisation	The process by which a directed surveillance operation is subject to proper consideration, recording and approval by the Officer conducting the investigation and the Officer authorised to approve it.
Authorising Officer	The suitably trained officers designated by the Council to authorise investigations under RIPA and IPA or obtain information from NAFN: • Chief Executive (Head of Paid Service) • Director of Governance & HR (Senior Responsible Officer' • Executive Director of Place & Economy • Executive Director of Adult, Community and Wellbeing; • Assistant Director, Regulatory Services
CHIS	Covert Human Intelligence Source is someone who: • establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the two bullet points below • covertly uses such a relationship to obtain information or to provide access to 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.

Collateral Intrusion	Intrusion into the privacy of persons other than those who are the direct subjects of the operational investigation, such as innocent bystanders. Unnecessary intrusion into the lives of those not directly involved in the operation will be avoided wherever possible. Before granting an authorisation, the Authorising Officer will take into account the possibility that similar surveillance activities are being undertaken by other public authorities.
Communications Data	Information relating to the use of a communications service, excluding the contents of the communication itself. Communications data can be split into three types: "service data" is the use made of the service by any person eg itemised telephone records; and "subscriber data" i.e. any other information that is held or obtained by an operator on a person they provide a service to. Local authorities are not allowed to access "traffic data" - i.e. where a communication was made from, to whom and when;
Confidential Information	Information which is legally privileged, personal information or confidential journalistic material
Covert Surveillance	Covert surveillance is defined in RIPA as any surveillance which is carried out in a manner calculated to ensure that the persons the subject of the surveillance are unaware that it is or may be taking place. RIPA goes on to define two different 'types' of covert surveillance: • directed surveillance • intrusive surveillance Intrusive surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device.
HRA	Human Rights Act 1998 - requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and their correspondence. This is a qualified right so in certain circumstances the Council may interfere in the citizen's right mentioned above, if such interference is: (a) in accordance with the law; (b) necessary; and (c) proportionate.
Investigating / Applying Officer	The suitably trained and authorised officers permitted to conduct enforcement investigations on behalf of the Council
IPA	Investigatory Powers Act – created the role of Investigatory Powers Commissioner, which replaced the Officer of Surveillance Commissioners as the body overseeing RIPA in local authorities

IPCO	Investigatory Powers Commissioners Office
Judicial Approval	An authorisation approved by an Authorising Officer is not valid until it has been approved by a Magistrate.
NAFN	National Anti-Fraud Network – a data and intelligence service providing a secure, single point of contact to access a wide range of information providers using robust legal gateways and processes that meet the highest standard of legislative compliance. Using NAFN services is considered good practice, demonstrating an appropriate level of due diligence and robust process involving verification, crime and/or debt recovery.
RIPA	Regulation of Investigatory Powers Act 2000 – the Act which extended to Local Authorities the ability to use directed surveillance, CHIS and access communication data, as well as appropriate safeguards.
SPOC	Single Point of Contact
Surveillance	- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications - recording anything mentioned above in the course of authorised surveillance - surveillance, by or with, the assistance of appropriate surveillance devices
URN	Unique Reference Number