Public Document Pack

Scan this QR code to see the meetings streamed by the Council

North East Derbyshire District Council

Our Ref:	AB/AJD
Contact:	Asher Bond
Tel:	01246 217375
Email:	Asher.bond@ne-derbyshire.gov.uk
Date:	Tuesday, 20 February 2024

To: **Members of the Standards Committee**

Please attend a meeting of the Standards Committee to be held on **Wednesday, 28 February 2024 at 2.00 pm in the Council Chamber**, District Council Offices, 2013 Mill Lane, Wingerworth, Chesterfield, S42 6NG.

Yours sincerely

Sarah Sternberg

Assistant Director of Governance and Monitoring Officer

Members of the Committee

Councillor K Gillott (Chair)
Councillor H Wetherall (Vice-Chair)
Councillor P Antcliff
Councillor C Cupit
Councillor P Kerry
Councillor F Petersen
Councillor K Rouse
G Hudson
A Orchard
D Richardson

For further information about this meeting please contact: Asher Bond 01246 217375

A G E N D A

1 Apologies for Absence

2 Declarations of Interest

Members are requested to declare the existence and nature of any disclosable pecuniary interests and/or other interests, not already on their register of interests, in any item in the agenda and withdraw from the meeting at the appropriate time.

3 Minutes of Last Meeting (Pages 4 - 6)

To note the Notes of the Informal Standards Committee held on 30 January 2024.

4 RIPA Policy Review and Social Media Guidance for Members - NOW PUBLISHED (Pages 7 - 45)

Report of the Assistant Director of Governance and Monitoring Officer.

5 Whistleblowing Policy Review - NOW PUBLISHED (Pages 46 - 63)

Report of the Assistant Director of Governance and Monitoring Officer.

6 Complaints Update (Pages 64 - 69)

Report of the Assistant Director of Governance and Monitoring Officer.

7 Work Plan (Page 70)

Report of the Assistant Director of Governance and Monitoring Officer.

8 Urgent Business (public session)

To consider any other matter which the Chair is of the opinion should be considered as a matter of urgency.

Access for All statement

You can request this document or information in another format such as **large print** or **language** or contact us by:

- **Phone** - *01246 231111*
- **Email** - *connectne@ne-derbyshire.gov.uk*
- **Text** - *07800 00 24 25*
- **BSL Video** *Call* – a three way video call with us and a BSL interpreter. It is free to call North East Derbyshire District Council with *Sign Solutions* or call into the offices at Wingerworth.
- Call with *Relay UK* via textphone or app on *0800 500 888*– a free phone service
- **Visiting** our *offices* at Wingerworth – 2013 Mill lane, *S42 6NG*

STANDARDS COMMITTEE

NOTES OF INFORMAL MEETING HELD ON TUESDAY, 30 JANUARY 2024

Present:

Councillor Kevin Gillott (Chair) (in the Chair)

Councillor Pat Kerry
Councillor Fran Petersen
Councillor Kathy Rouse

Also Present:

S Sternberg	Assistant Director of Governance and Monitoring Officer
A Maher	Governance Manager
A Bond	Governance Officer

STA/25/23-24 **Apologies for Absence**

Apologies for absence were received from Councillors P Antcliff, C Cupit and H Wetherall.

STA/26/23-24 **Minutes of Last Meeting**

RESOLVED – That the Minutes of the Standards Committee meeting held on 27 September and the Notes of the Standards Committee meeting held on 15 November 2023 be noted.

STA/27/23-24 **Review of the Constitution - Next Steps**

Committee were presented with a working document that highlighted typographical changes that had been made to the Council's Constitution. Committee considered that in future Officers should make these changes without the need to wait for approval from Committee. They heard that the Monitoring Officer had a delegation to this effect and would take the proposed approach going forward.

Members heard that the Constitution was currently divided into 29 sections. Officers had suggested that the Constitution could be split into two parts: Part One the Role of the Constitution and Part Two Technical Provisions supporting how Councillors and Officers work. Officers had attempted to identify what should form the core of the Constitution with additional documents and areas being treated as Constitutional Documents.

Committee considered that it would be worthwhile to have a core Constitution document separate from the appendices or Constitutional Documents as this would offer greater accessibility to Members.

Members heard that a further document could be created in order to make the Constitution more accessible to the wider public. This would be a concise, separate and simple document that would explain the role of the Council and

Councillors. This document could form the basis of a social media campaign or a further campaign aimed at targeting younger members of the public.

Committee considered that a common simple and accessible document could be worthwhile and heard that the Monitoring Officer would provide a document to the next meeting of Committee that would form the basis of this. Members also considered that there was a need to increase engagement with younger residents but that a wider social media campaign or public documents would not be a worthwhile use of resources.

Members discussed additional proposed changes to the Constitution. They asked for further information to be provided to them on the levels of the financial part of key decisions such as what has influenced this level and if any increase would be required due to factors such as inflation.

Committee agreed that the HOPS should be allowed to appoint on a higher point in the pay scale where the market is such that any appointment is difficult to achieve or for other good reason but that the Leader of the Council should be notified prior to this decision being taken.

Group agreed that the Monitoring Officer should be able to make or revoke appointments to outside bodies and make changes to the membership of Committees and Sub Committees following consultation with the relevant party Leader, the Leader and/or Deputy Leader of Council and the relevant Portfolio Holder. Group considered that after a change had been made, all Group leaders should be notified of the change.

Members considered that an Independent Remuneration Panel should be established to review the Members Allowance Scheme and that the same panel should also conduct a review at Rykneld Homes Ltd.

Committee discussed the procedure rules for meetings and considered that meetings of Full Council should be limited to a maximum duration of three hours with the option to extend the meeting following a vote to that effect.

Members drew attention to questions from the public and considered that a definition of who the public were should be included in the Constitution. It was agreed that the public, for these purposes, should be defined as electors, non domestic rate payers, 16/17 year olds who lived in the District and tax payers.

Members requested that the Monitoring Officer explore the possibility of limiting the wording of questions from members of the public at meetings of Council.

Committee considered Motions at meetings of Full Council and agreed that the Monitoring Officer should have the power to prevent any Motion that does not meet the correct criteria from being placed on the Agenda. Members also considered that when a Member seconds a Motion they should not be able to reserve their right to speak unless this is permitted by the Chair.

Members discussed rules at Planning Committee and asked the Monitoring Officer to investigate whether it was right and proper for full Council to be the

parent body for planning matters and what, if any, processes should be in place. They also asked that the Officer explore whether a Cabinet Member should sit on Planning Committee and what the planning and practical consequences would be of excluding people.

Committee considered that there were three grounds for dispensations that should be delegated to the Monitoring Officer. These were:

1. That, without the dispensation, the representation of different political groups on the body transacting the business would be so update as to alter the likely outcome of any vote on the matter.

2. That, without a dispensation, no member of the Cabinet would be able to participate in the matter.

3. That, so many members of the decision-making body have disclosable pecuniary interests in a matter that it would impede the transaction of the business.

North East Derbyshire District Council

Standards Committee

28th February 2024

Review of RIPA Policy

Report of the Assistant Director of Governance and Monitoring Officer

Classification**:** This report is public

Report By**:** Sarah Sternberg**,** Assistant Director of Governance and Monitoring Officer

Contact Officer: Sarah Sternberg**,** Assistant Director of Governance and Monitoring Officer

---

PURPOSE / SUMMARY

This report is part of the annual review of the Policy, a report on the use of the policy over the last year and an outline of the training to be provided to Authorising Officers and the applying officers in the next year.

RECOMMENDATIONS

1. To approve the RIPA policy as amended.

2. To receive the update on training, the statistics and a likely inspection.

IMPLICATIONS

Finance and Risk: **Yes☒** **No ☐**

Details:

There may be a cost to training but the real threat in finance terms is not following the procedure where required and a fine being imposed.

On Behalf of the Section 151 Officer

Legal (including Data Protection): **Yes☐** **No ☐**

Details:

As in the repot.

On Behalf of the Solicitor to the Council

Staffing: Yes☐ No ☐
Details:

None. This is part of the role of the Monitoring Officer and enforcement officers.

On behalf of the Head of Paid Service

DECISION INFORMATION

Decision Information	
Is the decision a Key Decision? A Key Decision is an executive decision which has a significant impact on two or more District wards or which results in income or expenditure to the Council above the following thresholds: **NEDDC:** **Revenue - £100,000 ☐ Capital - £250,000 ☐** ☒ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
District Wards Significantly Affected	None directly
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	Yes Details:

Links to Council Plan (NED) priorities, including Climate Change, Equalities, and Economics and Health implications.
This is about complying with statutory requirements for covert surveillance by enforcement officers of the Council. It is therefore covered by "A great place to access good public services"

REPORT DETAILS

1 Background *(reasons for bringing the report)*

1.1 This is the regular report on the review of the Regulation of Investigatory Powers Act Policy (RIPA) Policy and related matters. Under the Committee's terms of reference it is for Standards Committee to consider the report and approve any changes to the Policy

1.2 The Regulation of Investigatory Powers Act (RIPA) enables the Council to use covert surveillance; covert human intelligence sources (CHIS); and the acquisition of service use or subscriber information in relation to communications data in a manner that is compatible with Article 8 of the European Convention on Human Rights governing an individual's right to respect for their private and family life, home and correspondence. There are various criteria which must be met, including a 'seriousness threshold' for the use of directed surveillance, and any requests by the Council to use the RIPA powers must be approved by a Magistrate, under the current legislation.

1.3 Local authorities are sparing users of RIPA legislation and North East Derbyshire District Council has not used them since the last update to Committee in December 2022. The last time RIPA powers were utilised was in 2012.

2. Details of Proposal or Information

Inspection

2.1 The Council has been periodically inspected by the Office of Surveillance Commissioners in the past. The last inspection was in 2022. This was necessarily brief as the effects of the Covid Pandemic were still being felt. The outcome of the Inspection was overall very positive.

2.2 Inspections are now carried out by the Investigatory Powers Commissioner's Office (IPCO). Inspections of local authorities are scheduled for every three years, and so it is likely that there will be an inspection this year.

Authorisations

2.3 There have been no applications in the last year. This has been confirmed by the Authorising Officers (the Managing Director and Head of Paid Service, the Director of Growth and Assets and the Director of Finance and Resources and the Section 151 Officer). Most enforcement carried out by enforcement officers in the Council is overt and therefore outside RIPA.

Training

2.4 It is imperative that regular training is undertaken, as well as refresher sessions for officers involved in investigations as well as senior officers appointed as Authorising Officers and designated persons.

2.5 Training was last carried out by an external provider to Authorising and Applicant Officers in 2022. Training is therefore due for all potentially involved in the process. Therefore, refresher training will be carried out in 2024.

IPCO

2.4 As is the practice with breaches of the Data Protection rules, there is a requirement to report to IPCO any potential breaches of the RIPA rules or the Council's RIPA policy. I am not aware of any.

2.5 There is a requirement to report to IPCO once a year on the use of Covert surveillance and CHIS as covered by RIPA. This was completed in January 2024 with a nil return.

Use of drone in enforcement investigations

2.6 This is a developing area of potential use of drones, which officers are considering at the moment in terms of RIPA. A further report will be presented to Members when this work is complete and changes to the RIPA policy proposed if appropriate.

Non RIPA authorisations

2.6 None have been submitted in the last year.

RIPA pages

2.7 A new Extranet is being developed using Teams. This is not ready yet. Once it is, a new RIPA page will be developed with links to the Home Office guidance.

2.8 Similarly, the RIPA page on the website will also be reviewed to ensure it is up to date.

3 Reasons for Recommendation

Reasons for Recommendation

3.1 The RIPA policy has been reviewed to ensure it remains fit for purpose and it is concluded that the existing version is satisfactory and up to date with current legislation and best practise.

3.2 There have been no uses of the RIPA authorisation process to report to Members. As part of monitoring the use of RIPA, Members should be kept up to date with its use and therefore able to monitor its use.

4 Alternative Options and Reasons for Rejection

4.1 There are no alternatives to consider.

DOCUMENT INFORMATION

Appendix No	Title

1	RIPA Policy

Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet you must provide copies of the background papers)
None

North East Derbyshire District Council

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

CORPORATE POLICY AND PROCEDURES

Section: Introduction

CONTROL SHEET FOR REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) – CORPORATE POLICY AND PROCEDURES

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	RIPA Corporate Policy and Procedures
Current status – i.e. first draft, version 2 or final version	Final (2024 Review)
Policy author	AD Governance and Monitoring Officer
Location of policy – i.e. L-drive, shared drive	S Drive
Member route for approval	Standards Committee
Cabinet Member (if applicable)	Cllr J Birkin
Equality Impact Assessment approval date	July 2017
Partnership involvement (if applicable)	N/A
Final policy approval route i.e. Executive/ Council /Planning Committee	Standards Committee
Date policy approved	February 2024
Date policy due for review (maximum three years)	February 2025
Date policy forwarded to be included on Intranet and Internet if applicable to the public	

Contents

Abbreviations

AOs	Authorising Officers who are the Managing Director and Head Of Paid Service, Director of Finance and Resources and Section 151 Officer, Director of Growth and Assets.
CCTV	Closed Circuit Television
CSP	Communications service provider
Council	North East Derbyshire District Council
CHIS	Covert Human Intelligence Sources
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedom agreed on 2 November 1950
HRA	Human Rights Act 1998
ICCO	The Interception of Communications Commissioner's Office
IPCO	Investigatory Powers Commissioner's Office
NAFN	The National Anti Fraud Network
PFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SPoC's	Single Points of Contact for Acquisition and Disclosure of Communications Data

1.1 Introduction

1.1.1 This Corporate Policy and Procedures document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 and the Home Office's Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data.

1.1.2 The use of covert surveillance, covert human intelligence sources and the acquisition of service use or subscriber information in relation to communications data is sometimes necessary to ensure effective investigation and enforcement of the law. However, they should be used only rarely and in exceptional circumstances. RIPA requires that public authorities follow a clear authorisation process prior to using these powers. Authorisations granted under Part II of RIPA are subject to all the existing safeguards considered necessary by Parliament to ensure that investigatory powers are exercised compatibly with the ECHR.

1.1.3 <u>Any potential use of RIPA should be referred to the Monitoring Officer for preliminary advice at the earliest possible opportunity. In the Monitoring Officer's absence, advice should be sought from the Legal Team.</u>

Consequences of Failing to Comply with this Policy

1.1.4 Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA and this Policy may result in the Council's actions being deemed unlawful by the Courts under Section 6 of the HRA or by the Investigatory Powers Tribunal, opening up the Council to claims for compensation and loss of reputation. Additionally, any information obtained that could be of help in a prosecution may be inadmissible.

1.2 Background

1.2.1 On 2 October 2000 the Human Rights Act 1998 ("HRA") made it unlawful for a local authority to breach any article of the ECHR. An allegation that the Council or someone acting on behalf of the Council has infringed the ECHR is dealt with by the domestic courts rather than the European Court of Justice.

1.2.2 The ECHR states:-

(a) individuals have the right to respect for their private and family life, home and correspondence (Article 8 ECHR); and

(b) there shall be no interference by a public authority with the exercise of this right unless that interference is:-

- **in accordance with the law;**
- **necessary; and**
- **proportionate**

1.2.3 RIPA, which came into force on 25 September 2000, provides a lawful basis for three types of covert investigatory activity to be carried out by local authorities which activities might otherwise breach the ECHR. These activities are:-

- covert directed surveillance;
- covert human intelligence sources ("CHIS"); and
- acquisition and disclosure of communications data

1.2.4 RIPA sets out procedures that must be followed to ensure the investigatory activity is lawful. Where properly authorised under RIPA the activity will be a justifiable interference with an individual's rights under the ECHR. If the interference is not properly authorised an action for breach of the HRA could be taken against the Council, a complaint of maladministration made to the Local Government Ombudsman or a complaint made to the Investigatory Powers Tribunal. In addition, if the procedures are not followed any evidence collected may be disallowed by the courts. RIPA seeks to balance the rights of individuals against the public interest in the Council being able to carry out its statutory duties.

1.2.5 A flow chart attached at Appendix A to this policy sets out the process for covert directed surveillance and covert human intelligence sources (CHIS).

What RIPA Does and Does Not Do

1.2.6 RIPA does:-

- require prior authorisation of covert directed surveillance;
- prohibit the Council from carrying out intrusive surveillance;

- compel disclosure of communications data from telecom and postal service providers;
- permit the Council to obtain communications records from communications service providers;
- require authorisation of the conduct and use of CHIS;
- require safeguards for the conduct of the use of a CHIS.

1.2.7 RIPA does not:-

- make conduct unlawful which is otherwise lawful;
- prejudice any existing power to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the Council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a property;
- apply to activities outside the scope of Part II of RIPA. A public authority will only engage RIPA when in performance of its "core functions" – i.e. the functions specific to that authority as distinct from all public authorities.
- cover overt surveillance activity.

1.2.8 RIPA only applies to the Council's core functions – i.e. its statutory duties, and not staffing issues or contractual disputes.

1.2.9 Under no circumstances can local authorities be authorised to obtain communications traffic data under RIPA. Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

1.3 Policy Statement

1.3.1 The Council is determined to act responsibly and in accordance with the law. To ensure that the Council's RIPA activity is carried out lawfully and subject to the appropriate safeguards against abuse, a Corporate Policy and Procedures document has been drafted as detailed below.

1.3.2 All staff who are considering undertaking RIPA activity should be aware that where that activity may involve handling confidential information or the use of vulnerable or juvenile persons as sources of information, a higher level of authorisation is required. Please see paragraphs 2.7 (in respect of handling confidential information) and 2.9 (in respect of using information sources who are vulnerable or juvenile persons) below.

1.3.3 The following information and documents are available ~~on the Council's Extranet~~:-

- Home Office Statutory Codes of Practice on the Gov.uk website.
- ~~Links to Office of the Surveillance Commissioners' Guidance Procedures online~~
- Links to RIPA forms online for covert surveillance; CHIS and acquisition and disclosure of communications data;
- Corporate RIPA Training.

1.3.4 The Monitoring Officer is the Council's Senior Responsible Officer (SRO) and is responsible for the following roles:-

- Appointing Authorising Officers (see 2.11);
- Appointing Designated Persons (see 3.4);
- Maintaining a central record for all RIPA authorisations;
- Arranging training to individuals appointed as Authorising Officers and Designated Persons, and
- Carrying out an overall monitoring function as the SRO for the Council's use of RIPA powers.

1.3.5 Any officers who are unsure about any RIPA activity should contact the Monitoring Officer for advice and assistance.

1.3.6 Where surveillance activity is carried out in relation to crimes that do not meet the RIPA Thresholds as detailed within this policy, these must be logged within individual Council departments and submitted to the Monitoring Officer on a quarterly basis. Non-RIPA Authorisations will be considered by Members as part of their Annual Report.

1.4 Social Media

1.4.1 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Although information that individuals make publically available on the internet would not normally be classed as 'private information', the Office of the Surveillance Commissioners' Annual Report 2016 states that repeated visits to individual sites may develop into surveillance activity which would require authorisation. By virtue of conducting research online, rather than using other more 'overt' methods, there may be a perception that the investigation is intended to be covert. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights. Particular consideration should be paid to the likelihood of collateral intrusion through obtaining private information about others who have not given their consent. Advice should be sought as early as possible.

1.4.2 Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and be proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

1.4.3 The Council maintains detailed and specific guidance for its officers' use of social media in investigations. This forms an annex to this policy and should be referred to in all circumstances where:

- open source research is gathered;
- open source information is publically available; and

- Information is stored for an investigation.

1.4.4 The Council does not ordinarily permit the use of false personas to obtain information. Any such need to do so requires the authorisations detailed in Section 2.

1.5 Training & Advice and Departmental Policies, Procedures and Codes of Conduct

1.5.1 The Monitoring Officer will arrange regular training on RIPA. All Authorising Officers, designated persons and investigating officers should attend at least one session every two years and further sessions as and when required.

1.5.2 Training can be arranged on request and requests should be made to the Monitoring Officer. In particular training should be requested for new starters within the Council who may be involved in relevant activities.

1.5.3 If officers have any concerns, they should seek advice about RIPA from the Monitoring Officer.

1.5.4 Where in practice, departments have any policy, procedures or codes of practice in relation to RIPA that are different from or in addition to this Code, they must immediately seek advice from the Monitoring Officer.

1.6 Complaints

1.6.1 Any person who believes they have been adversely affected by surveillance activity or other investigatory activity covered by RIPA by or on behalf of the Council may complain to the authority.

1.6.2 They may also complain to the Investigatory Powers Tribunal at:-

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

1.7 Monitoring of Authorisations

1.7.1 The Monitoring Officer is the senior responsible officer in relation to RIPA and is responsible for:-

- The integrity of the process in place to authorise directed surveillance, the use of CHIS and the acquisition and disclosure of communications data;
- Compliance with Part II of RIPA and this Policy;
- Engagement with the Investigatory Powers Act Commissioner's Office when they conduct inspections; and
- Where necessary, overseeing the implementation of any post-inspection plans recommended or approved by a Commissioner.

1.7.2 The Monitoring Officer is also required by law to ensure that the Council does not act unlawfully and will undertake audits of files to ensure that RIPA is being complied with and will provide feedback to the Authorising Officer/designated person where deficiencies in the RIPA process are noted.

1.7.3 The Monitoring Officer will invite the Standards Committee to review the Council's RIPA Policy on an annual basis and to recommend any changes to the Council's Policy or Procedures and will also provide members with an annual update on use.

1.8 Error Reporting

1.8.1 The Council is required to report 'relevant errors' to the Investigatory Powers Commissioner, which includes circumstances where the requirements of the RIPA legislation or guidance have not been met. Examples include:

- Surveillance activity has taken place without lawful authorisation
- There has been a failure to adhere to the safeguards applicable to the use of a CHIS.

1.8.2 When any officer identifies that activity that should have been authorised under RIPA may have taken place, they must notify the Monitoring Officer immediately. The officer(s) involved in the investigation will be required to provide a report on all relevant circumstances including:

- Information on the cause of the potential error
- The amount of surveillance or property interference conducted
- Nature and amount of any material obtained or disclosed
- Details of any collateral intrusion (i.e. any third party information collected in addition to that of the subject of the investigation.)
- Whether any material has been retained or destroyed

1.8.3 The Monitoring Officer will determine whether a 'relevant error' has occurred. If required, the Monitoring Officer will also give advice on steps to be taken to avoid the error recurring.

1.8.4 If the Monitoring Officer establishes that a 'relevant error' has occurred, this must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable and no later than 10 days after the error has been established. If additional time is required to ascertain the full facts of the error, an initial notification must be submitted with an estimated timetable of when the full report can be supplied.

1.8.5 The report to the Investigatory Powers Commissionioner must contain the details set out at 1.8.2 as well as details of any steps taken to prevent recurrence of the error.

1.8.6 If an authorisation has been obtained on the basis of information provided by a third party that later turns out to be incorrect, but was relied upon in good faith, this error should also be notified to the Investigatory Powers Commissioner (although it does not constitute a 'relevant error' under the legislation).

1.8.7 The Home Office Guidance sets out what action the Investigatory Powers Commissioner will take following notification of relevant errors, including determining whether it is a serious error and whether the person concerned should be notified.

1.8.8 The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but was not. This is to confirm that any direction provided by the Commissioner has been followed.

RIPA PART 2

COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

2.1 Types of Surveillance

2.1.1 Surveillance can be overt or covert and includes:-

- 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 device.*

*More detailed guidance on the use of surveillance devices, such as cameras, microphones, vehicle tracking and drones can be found in the relevant Home Office Code of Practice.

2.1.2 Indicators of whether investigatory activity will amount to surveillance include the formality and duration of the activity and the nature of what is being observed.

2.2 Overt Surveillance

2.2.1 The majority of the Council's surveillance activity will be overt surveillance, i.e. will be carried out openly. For example (i) where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted; and (ii) where the Council advises a tenant that their activities will be monitored as a result of neighbour nuisance allegations. This type of overt surveillance is normal Council business and is not regulated by RIPA.

2.3 Covert Surveillance

2.3.1 This is where surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware it is taking place. Covert surveillance can be intrusive or directed. **The Council is not permitted to carry out covert intrusive surveillance.** Para 2.4 below explains when covert surveillance is intrusive and therefore not permitted. The Council is permitted to carry out covert directed surveillance subject to strict compliance with RIPA. Paragraph 2.5 below explains when covert surveillance is directed.

2.4 Covert Intrusive Surveillance

2.4.1 Covert intrusive surveillance takes place when covert surveillance is carried out in relation to anything taking place on residential premises or in a private vehicle and which involves the presence of an individual or surveillance device on the premises or in the vehicle, or which uses a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as expected of a device placed inside. Additionally, the Regulation of Investigatory Powers

(Extension of Authorisations Provisions: Legal Consultations) Order 2010 states that covert surveillance carried out in relation to anything taking place in certain specified premises is intrusive when they are being used for legal consultation.

2.5 Covert Directed Surveillance

2.5.1 This is surveillance that is:-

- Covert;
- Not intrusive;
- For the purposes of a specific investigation or operation;
- Likely to obtain private information* about a person (whether or not that person was the target of the investigation or operation); and
- Not carried out as an immediate response to events or circumstances which could not have been foreseen prior to the surveillance taking place.

* Private information includes any information relating to a person's private and family life including professional and business relationships, home and correspondence (whether at home, in a public place or in the work place). Further information and examples of what is considered private information is contained at section 3 of the Home Office Code of Practice on Covert Surveillance and Property Interference.

2.6 Directed Surveillance Crime Threshold

2.6.1 Following the changes to RIPA introduced by the Protection of Freedoms Act 2012, a crime threshold applies to the authorisation of covert directed surveillance by local authorities. *(Article 7A of Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010)*

2.6.2 Local Authority Authorising Officers may not authorise covert directed surveillance unless it is for the purpose of preventing or detecting a criminal offence **and** meets the following test:-

- The criminal offence is punishable by a maximum term **of at least six months imprisonment**, or

- It would constitute an offence under Sections 146, 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1993 **(offences involving sale of tobacco and alcohol to underage children)** regardless of length of prison term.

2.6.3 Whether or not the crime threshold is met should be kept under review during the course of the investigation. If the relevant criminal offence is downgraded and the threshold is no longer met, the authorisation for surveillance should be cancelled.

2.6.4 The crime threshold **only** applies to covert directed surveillance, not to CHIS or Communications Data.

2.6.5 The Home Office Statutory Covert Surveillance and Property Interference Code of Practice can be found on the Home Office website.

2.7 Confidential Information

2.7.1 A higher level or authorisation to apply to the Magistrates Court is required in relation to RIPA activity when the subject of the investigation might reasonably expect a high degree of privacy, or where "confidential information" might be obtained. For the purpose of RIPA this includes:-

- Communications subject to legal privilege (see below);
- Communications between a member of parliament and another person on constituency matters;
- Confidential personal information (see below); and
- Confidential journalistic material (see below).

2.7.2 The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure. **Authorisation can only be granted by the Head of Paid Service**.

2.7.3 **Legal privilege** is defined in Section 98 of the Police Act 1997 as:-

- communications between a professional legal adviser and his client, or any person representing his client which are made in connection with the giving of legal advice to the client.

- communications between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

- items enclosed with or referred to in communications of the kind mentioned above and made in connection with the giving of legal advice, or in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

2.7.4 Communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

2.7.5 If advice is required on this point, officers should contact the Monitoring Officer.

2.7.6 **Confidential personal information** is described at paragraph 4.28 of the Home Office Covert Surveillance and Property Interference Code of Practice.

2.7.7 **Confidential journalistic material** is described at paragraph 3.40 of the Home Office Covert Surveillance and Property Interference Code of Practice.

2.7.8 **Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from the Monitoring Officer prior to making any application.**

2.8 Covert Human Intelligence Sources ("CHIS")

2.8.1 The Council is permitted to use CHIS subject to strict compliance with RIPA.

A CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purposes of facilitating:-

(a) covertly using the relationship to obtain information or provide access to information to another person, or

(b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.

2.8.2 A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf. Authorisation for CHIS can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder".

2.8.3 Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

2.8.4 However, by virtue of Section 26(8) of RIPA, there may be instances where an individual, covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship. In such circumstances where a member of the public, though not asked to do so, gives information (or repeated information) about a suspect, then serious consideration should be given to designating the individual as a CHIS, particularly if the Council intends to act upon the information received. It is recommended that legal advice is sought in any such circumstances.

2.9 Safety and Welfare of CHIS

2.9.1 The safety and welfare of the CHIS is paramount. Risk assessments should be carried out to determine the risk of tasking a CHIS and the activities being undertaken by the particular person appointed. The risk assessments should be regularly reviewed during the course of the investigation.

2.9.2 A single point of contact should be appointed for the CHIS to communicate with, who will be responsible for carrying out the risk assessments and taking all possible steps to ensure their safety and welfare. A senior officer should also have oversight of the arrangements and be regularly updated by officer acting as the single point of contact. Regular face-to-face meetings should occur with the CHIS rather than solely

remote contact, such as telephone or email, although remote contact may be appropriate in addition.

2.10 Vulnerable Individuals/Juvenile CHIS

2.10.1 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves or protect themselves against significant harm or exploitation.

2.10.2 Additional requirements apply to the use of a vulnerable adult or a person under the age of 18 as a CHIS. In both cases **authorisation for an application to the Magistrates Court can only be granted by the Head of Paid Service. Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the Monitoring Officer prior to making the application.**

2.10.3 The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them. In other cases authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. This set out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

2.11 CCTV

2.11.1 The installation and use of unconcealed CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance requiring RIPA authorisation. There are specific provisions relating to the use of CCTV cameras in public places and buildings. However, if CCTV cameras are being used in such a way that the definition of covert directed surveillance is satisfied, RIPA authorisation should be obtained.

2.11.2 For instance the use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation. However, the use of the same CCTV system to conduct planned surveillance of an individual and record their movements is likely to require authorisation.

2.11.3 Protocols should be agreed with any external agencies requesting the use of the Council's CCTV system. The protocols should ensure that the Council is satisfied that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

2.11.4 CCTV systems cannot be used without prior production of an authorisation and such authorisations must be retained.

2.12 Authorisation Procedures

Authorisations given by Authorising Officers are subject to approval by the Magistrates Court (See para 2.15 below)

2.12.1 Authorising Officers are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

2.12.2 It is the responsibility of Authorising Officers to ensure that when applying for authorisation the principles of necessity and proportionality (see 2.13 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (2.20 – 2.22 below).

2.12.3 Lists of Authorising Officers are set out below. Any requests for amendments to the lists must be sent to the Monitoring Officer.

2.12.4 The authorising officers for North East Derbyshire District Council are as follows:

Managing Director & Head of Paid Service – Lee Hickin (01246 217218)

Director of Finance and Resources – Jayne Dethick (01246 2417078)
Director of Growth and Assets – Matthew Broughton (01246 242210)

2.12.5 Schedule 1 of statutory instrument No 521 (2010) prescribes the rank or position of authorising officers for the purposes of Section 30(1) of RIPA (covert surveillance and CHIS). For Local Authorities they prescribe a “Director, Head of Service, Service Manager or equivalent”.

2.12.6 The Monitoring Officer designates which officers can be Authorising Officers. Only these officers can authorise directed surveillance and the use of CHIS. **All authorisations must follow the procedures set out in the Policy**. Authorising officers are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the Monitoring Officer.

2.13 Authorisation Of Covert Directed Surveillance And Use Of A CHIS

2.13.1 RIPA applies to all covert directed surveillance and the use of CHIS whether by Council employees or external agencies engaged by the Council. Council officers wishing to undertake covert directed surveillance or use of a CHIS must complete the relevant application form and forward it to the relevant (para 2.11.4) Authorising Officer.

2.13.2 Any potential use of RIPA should be referred to the Monitoring Officer for preliminary advice.

2.14 Criteria For The Authorisation Of The Use Of RIPA Powers

2.14.1 Covert directed surveillance and/or the use of a CHIS can only be authorised if the Authorising Officer is satisfied that the activity is:-

(a) **in accordance with the law** i.e. it must be in relation to matters that are statutory or administrative functions of the Council. As such the Council is unable to access communications data for disciplinary matters.

(b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and for directed surveillance only, there is a crime threshold as described in paragraph 2.6 above;

(c) **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct, or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

2.14.2 Applicants should ask the following types of questions to help determine whether the use of RIPA is necessary and proportionate:-

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate);
- how the activity to be authorised is expected to bring a benefit to the investigation;
- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation;
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the ECHR;
- what other reasonable methods of obtaining information have been considered and why they have been discounted.

2.14.4 When completing an application, officers must present the case in a fair and balanced way. In particular all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation.

2.14.4 Authorising Officers should not be responsible for authorising their own activities, i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable. The Monitoring Officer should be informed in such cases.

2.14.5 Particular consideration should be given to **collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation.** Collateral intrusion occurs when an officer undertaking covert surveillance on a

subject observes or gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into account by the authorising officer, particularly when considering the proportionality of the surveillance.

2.14.6 Particular care must be taken in cases where **confidential information** is involved e.g. matters subject legal privilege, confidential personal information, confidential journalistic material, confidential medical information, and matters relating to religious leaders and their followers. In cases where it is likely that confidential information will be acquired, officers must specifically refer this to the Monitoring Officer for advice.

2.15 Processing the authorisation

2.15.1 At the time of authorisation the Authorising Officer must set a date for review of the authorisation and review it on that date (see 2.19), prior to authorisation lapsing as it must not be allowed to lapse.

2.15.2 The original completed application and authorisation form must be forwarded to the Monitoring Officer as soon as possible. The Monitoring Officer will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application. This will be kept in Legal Services.

2.16 Approval by Magistrates Court

2.16.1 Under the Protection of Freedoms Act 2012, there is an additional stage in the process for investigatory activities (covert directed surveillance and CHIS). After the authorisation form has been countersigned by the Authorising Officer, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

2.16.2 The Council has a protocol for the Magistrates' approval process, including out of hours procedures, which is held by the Legal Team.

2.16.3 The magistrate will have to decide whether the Council's application to grant or renew an authorisation to use RIPA should be approved and it will not come into effect unless and until it is approved by the Magistrates Court.

2.16.4 *A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the surveillance techniques (i.e. Directed Surveillance, CHIS and Communications Data) at the same time.*

2.16.5 It should be noted that only the initial application and any renewal of the application require magistrates' approval.

2.16.6 There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified but they do need to be authorised by the Council to

represent it in court. **Generally the applicant should be accompanied to Court by the Authorising Officer and a member of the legal team.**

2.17 The Role of the Magistrates Court

2.17.1 The role of the Magistrates Court is set out in Section 32A RIPA (for directed surveillance and CHIS).

2.17.2 This section provide that the authorisation shall not take effect until the Magistrates Court has made an order approving such authorisation. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:-

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate;

- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:

    - arrangements exist for the safety and welfare of the source that satisfy Section 29(5) RIPA;
    - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied;

- The local authority application has been authorised by an authorising officer;

- The grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
    - 29(7)(a) (for CHIS),
    - 30(3) (for directed surveillance and CHIS).

Summary of procedure for applying for covert directed surveillance or use of a CHIS is:

- Applicant obtains preliminary legal advice from Monitoring Officer;
- Applicant completes an application;
- Monitoring Officer quality checks the completed application before organising it to go to the Authorising Officer;
- Approval is sought from the Authorising Officer;
- Authorising Officer completes authorisation form in long-hand;
- Monitoring Officer organises paperwork for court and the applicant, the Authorising Officer proceeds to court, accompanied by a member of the legal team wherever possible;
- If approval given, applicant organises the covert directed surveillance or use of a CHIS to take place;
- Original copy of application lodged with Legal Team.

Additional Requirements for Authorisation of a CHIS

A CHIS must only be authorised if the following arrangements are in place:-

- There is a Council officer with day-to-day responsibility for dealing with the CHIS and a senior Council officer with oversight of the use made of the CHIS;
- A risk assessment has been undertaken to take account of the CHIS security and welfare;
- A Council officer is responsible for maintaining a record of the use made of the CHIS;
- Any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating; and
- Records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS.

2.17 Urgent Authorisations

2.17.1 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are not available.

2.18 Application Forms

2.18.1 Only the RIPA Forms listed below can be used by officers applying for RIPA authorisation.

(a) Directed Surveillance

- Application for Authority for Directed Surveillance
- Review of Directed Surveillance Authority
- Cancellation of Directed Surveillance
- Renewal of Directed Surveillance Authority

(b) CHIS

- Application for Authority for Conduct and Use of a CHIS
- Review of Conduct and Use of a CHIS
- Cancellation of Conduct and Use of a CHIS
- Renewal of Conduct and Use of a CHS

2.19 Duration of the Authorisation

2.19.1 Authorisation/notice durations are:-

- for covert directed surveillance the authorisation remains valid for three months after the date of authorisation;
- for a CHIS the authorisation remains valid for 12 months after the date of authorisation (or after four month if a juvenile CHIS is issued);

2.19.2 Authorisations should not be permitted to expire, they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that all authorisations must be reviewed to decide whether to cancel or renew them.

2.20 Review of Authorisations

2.20.1 As referred to at 2.11.2 and 2.14.1 Authorising Officers must make arrangements to periodically review any authorised RIPA activity. Officers carrying out RIPA activity, or external agencies engaged by the Council to carry out RIPA activity, must periodically review it and report back to the Authorising Officer if there is any doubt as to whether it should continue. Reviews should be recorded on the appropriate Home Office Form (see 2.18).

2.20.2 A copy of the Council's notice of review of an authorisation must be sent to the Monitoring Officer as soon as possible to enable the central record on RIPA to be authorised.

2.21 Renewal of Authorisations

2.21.1 If the Authorising Officer considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained, considering the same criteria as for new applications (see 2.13 above). Renewed authorisations will normally be for a period of up to three months for covert directed surveillance or 12 months in the case of CHIS, one month in the case of juvenile CHIS. Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation. Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form (see 2.18).

2.21.2 All renewals will require an order of the Magistrates Court in accordance with the requirements in para 8.2 above.

2.21.3 A copy of the Council's notice of renewal of an authorisation must be considered by the Monitoring Officer before it is made and all original copies lodged with the Legal Team together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

2.22 Cancellation of Authorisations

2.22.1 The person who granted or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance or CHIS no longer meets the criteria for authorisation. Cancellations must be made on the appropriate Home Office Form (see 2.18).

2.22.2 A copy of the Council's notice of cancellation of an authorisation must be sent to the Monitoring Officer within one week of the cancellation to enable the central record on RIPA to be updated.

2.23 What happens if the surveillance has unexpected results?

2.23.1 Those carrying out the covert surveillance should inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

2.24 Records and Documentation

Departmental Records

2.24.1 Applications, renewals, cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

Central Record of Authorisations, Renewals, Reviews and Cancellations

2.24.2 A joint central record of directed surveillance and CHIS is maintained by the Monitoring Officer at the District Council Offices, Mill Lane, Wingerworth.

2.24.3 The central record is maintained in accordance with the requirements set out in the Home Office Codes of Practice. In order to keep the central record up-to-date Authorising Officers must, in addition to sending through the Home Office application, authorisation form and Magistrates Court order as soon as possible following the authorisation being approved by the Magistrates Court (see 2.15) send notification of every renewal, cancellation and review on the Council's notification forms (see 2.19 – 2.22).

2.24.4 Using the information on the central record the Monitoring Officer will:-

- remind Authorising Officers in advance of the expiry of authorisations;
- remind Authorising Officers of the need to ensure surveillance does not continue beyond the authorised period;
- remind Authorising Officers to regularly review current authorisations;
- on the anniversary of each authorisation, remind Authorising Officers/delegated persons to consider the destruction of the results of surveillance operations.

2.25 Surveillance products

2.25.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

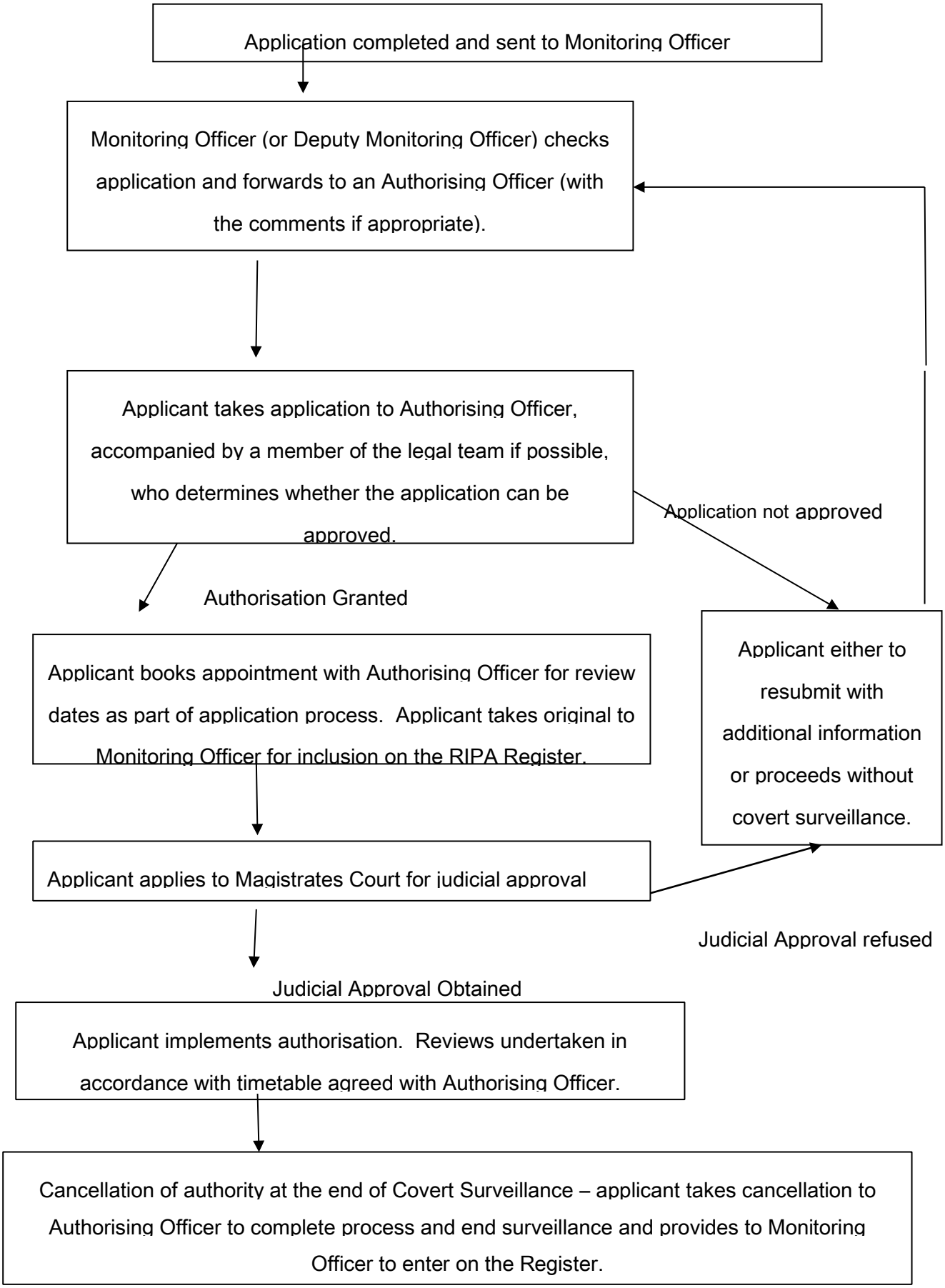
2.25.2 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996 by the Home Office and on the Home Office website. These requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

2.25.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use of covert surveillance to facilitate its use in other investigations.

2.25.4 Material obtained through the use of directed surveillance or CHIS containing personal information will be protected by the Data Protection Act 2018 (DPA) and in addition to the considerations above must be used, stored and destroyed in compliance with the appropriate requirements of the DPA and the Council's Data Protection, Information Security and Records Management Policies.

2.25.5 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. See section 9 of the Home Office Code of Practice for more detail of the safeguards that must be in place. Particular protection must be given to confidential or privileged information.

APPENDIX A - RIPA PROCESS



RIPA PART 1 – CHAPTER 2
ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

3.1 Permitted Purposes for Acquisition and Disclosure of Communications Data

3.1.1 Local authorities are only permitted to acquire communications data for the purposes of preventing or detecting serious crime. Other purposes are permitted for other public bodies.

3.1.2 A 'serious crime' is an offence that is punishable by a maximum term of imprisonment of 12 months or more.

3.1 Communication Service Providers ("CSPs")

3.1.1 CSPs are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also, for example, hotel or library staff involved in providing and maintaining email access to customers. The Council must obtain communications data from CSPs in strict compliance with RIPA.

3.2 Types of Communications Data

3.2.1 Communications data is the "who", "where", "when" and "how" of a communication such as a letter, phone call or email but not the content, not what was said or written. The Council is not able to use RIPA to authorise the interception or acquisition of the content of communications. There are three types of communication data:-

Service Use Information

3.2.2 This is data relating to the use made by any person of a postal or telecommunications, internet service, or any part of it. For example itemised telephone call records, itemised records of connection to internet services, itemised timing and duration of calls, connection/disconnection/reconnection data, use of forwarding or re-direction services, additional telecom services and records of postal items.

Subscriber information

3.2.3 This is information held or obtained by the CSP about persons to whom the CSP provides or has provided a communications service. For instance, subscribers of email and telephone accounts, account information including payment details, address for installing and billing, abstract personal records and sign up data.

Traffic Information

3.2.4 This is data that is comprised in or attached to a communication for the purpose of transmitting it and which identifies a person or location to or from which it is transmitted. **The Council is not permitted to access traffic data.**

3.3 Authorisation and Notices

3.3.1 RIPA provides for acquisition and disclosure of communications data by two alternative means:-

- authorisation of a person within the Council to engage in specific conduct, in order to obtain communications data (a section 22(3) RIPA authorisation); and

- a notice issued to a CSP requiring them to collect or retrieve and then provide the communications data (a section 22(4) RIPA notice).

3.3.2 A Section 22(3) RIPA authorisation is appropriate where (for instance) there is an agreement in place between the Council and the relevant CSP regarding the disclosure of communications data which means a notice is not necessary (currently the Council does not have any such agreements in place); or the Council needs to identify an individual to whom communication services are provided but the relevant CSP is not yet known to the Council, making it impossible to issue a notice.

3.3.3 A Section 22(4) RIPA notice is appropriate where the Council receives specific communications data from a known CSP. A notice may require a CSP to obtain any communications data, if that data is not already in its possession. However, a notice must not place a CSP under a duty to do anything which is not reasonably practicable for the CSP to do.

3.3.4 As a local authority the Council must fulfil two additional requirements when acquiring communications data. Firstly, in accordance with the Home Office Acquisition and Disclosure of Communications Data Code of Practice, the request must be made through a qualified Single Point of Contact (see more at 3.5 and 3.8). Secondly, the request must receive prior judicial approval.

3.3.5 Under Sections 23A and 23B of RIPA the Council must obtain judicial approval for all requests for communications data. Judicial approval must be requested once all the Council's internal authorisation processes have been completed, including consultation with a NAFN SPoC, but before the SPoC requests the data from the CSP. The authorisation must be provided by a magistrate.

3.3.6 The Home Office Acquisition and Disclosure of Communications Data Code of Practice can be found on the Home Office website and on the intranet.

3.4 Authorisation Procedures

Authorisations given by Designated Persons are subject to approval by the Magistrates Court (See para 3.10 below)

3.4.1 Designated Persons are responsible for considering applications for obtaining communications data, assessing and approving authorisations and notices.

3.4.2 It is the responsibility of Designated Persons to ensure that when applying for authorisation the principles of necessity and proportionality (see 3.8.2 and 2.14)

are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (3.14 – 3.17 below).

3.4.3 The list of designated persons is set out below. Any requests for amendments to the lists must be sent to the Monitoring Officer.

3.4.4 The designated persons for North East Derbyshire District Council are as follows:

Managing Director and Head of Paid Service – Lee Hickin
Director of Finance and Resources and Section 151 Officer – Jayne Dethick
Director of Growth and Assets – Matthew Broughton

3.4.5 Schedule 2 of statutory instrument No 480 (2010) prescribes the rank or position of designated person for the purposes of Section 25(2) of RIPA (access to communications data). For Local Authorities they prescribe a "Director, Head of Service, Service Manager or equivalent".

3.4.6 The Monitoring Officer designates which officers can be designated persons. Only these officers can authorise the acquisition and disclosure of Communications data. **All authorisations must follow the procedures set out in the Policy**. Designated persons are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the Monitoring Officer.

3.5 Authorisation of Acquisition and Disclosure of Communications Data

3.5.1 Any potential use of RIPA should be referred to the Monitoring Officer for preliminary advice.

3.5.2 RIPA applies to all acquisition and disclosure of communications data whether by Council employees or external agencies engaged by the Council. Authorisations or notices in relation to communications data should be referred to NAFN.

3.5.3 The rules on the granting of authorisations for the acquisition of communications data are slightly different from directed surveillance and CHIS authorisations and involve three roles within the Council. The roles are:-

- Applicant
- Designated Person
- Single Point of Contact

3.6 Applicant

3.6.1 This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The application form must:-

- Set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of serious crime;
- Describe the communications data required i.e. the telephone number, email address, the specific date or period of the data and the type of data required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted.
- Explain why the conduct is necessary and proportionate.
- Consider and describe any meaningful collateral intrusion. For example, where access is for "outgoing calls" from a "home telephone" collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it.

3.7 Designated Person

3.7.1 This is the person who considers the application. A designated person's role is the same as an Authorising Officer's role in relation to directed surveillance and CHIS authorisations. The designated person assesses the necessity for any conduct to obtain communications data taking account of any advice provided by the single point of contact (SPoC). If the designated person believes it is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

3.7.2 The Designated Person must refer the criteria set out at paragraph 2.14, as the same principles of necessity and proportionality apply to the use of cover directed surveillance and CHIS.

3.7.3 Designated persons should not be responsible for authorising their own activities, i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable. The Monitoring Officer should be informed in such cases.

3.7.4 Particular consideration should be given to **collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation.** Collateral intrusion occurs when an officer gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into account by the designated person, particularly when considering the proportionality of the surveillance.

3.7.5 Particular care must be taken in cases where **confidential information** is involved e.g. matters subject legal privilege, confidential personal information, confidential journalistic material, confidential medical information, and matters relating to religious leaders and their followers. In cases where it is likely that confidential

information will be acquired, officers must specifically refer this to the Monitoring Officer for advice.

3.7.6 At the time of authorisation the designated person must set a date for review of the authorisation and review it on that date (see 3.1 and 3.15), prior to authorisation lapsing as it must not be allowed to lapse.

3.7.7 The original completed application and authorisation form must be forwarded to the Monitoring Officer as soon as possible. In the case of a section 22(4) RIPA notice requiring disclosure of communications data a copy of the notice must be attached to the application form. The Monitoring Officer will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application.

3.8 Single Point of Contact (SPoC)

3.8.1 SPoCs are responsible for advising officers within the Council on how best to go about obtaining communications data, for liaising with CSPs, and advising whether applications and notices are lawful. As required under the latest Acquisition and Disclosure of Communications Data Code of Practice, the Council has engaged the National Anti-Fraud Network (NAFN). NAFN's SPoC services relate only to communications data.

3.8.2 More details on NAFN are available at www.nafn.gov.uk

3.9 Approval by Magistrates Court

3.9.1 Under the Protection of Freedoms Act 2012, there is an additional stage in the process for the acquisition of communications data. After the authorisation form has been countersigned by the designated person, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

3.9.2 The Council has a protocol for the Magistrates' approval process, including out of hours procedures, which is held by the Legal Team.

3.9.3 The magistrate will have to decide whether the Council's application to grant or renew an authorisation to use RIPA should be approved and it will not come into effect unless and until it is approved by the Magistrates Court.

3.9.4 A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the surveillance techniques (i.e. Directed Surveillance, CHIS and Communications Data) at the same time.

3.9.5 It should be noted that only the initial application and any renewal of the application require magistrates' approval.

3.9.6 There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified but they do need to be authorised by the Council to

represent it in court. **Generally the applicant should be accompanied to Court by the designated person and a member of the legal team.**

3.10 The Role of the Magistrates Court

3.10.1 The role of the Magistrates Court is set out in Section 23A RIPA (for communications data).

3.10.2 These sections provide that the notice, shall not take effect until the Magistrates Court has made an order approving such notice. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:-

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate;
- The local authority application has been authorised by a designated person;
- The grant of the notice was not in breach of any restriction imposed by virtue of an order made under sections 25(3) (for communications data) of RIPA:

Summary of procedure for applying for acquisition of communications data:

- Applicant obtains preliminary legal advice from Monitoring Officer;
- Applicant officer creates an application using the Cycomms Web Viewer on the NAFN website;
- SPoC Officer at NAFN triages and accepts the application into the Cyclops system;
- SPoC Officer uses Cyclops to update the application details and completes the SPoC report;
- Approval is sought from the Designated Person (DP);
- If approval given, Monitoring Officer organises paperwork for court and the applicant and the DP proceeds to court, accompanied by a member of the legal team wherever possible;
- SPoC receives signed court documents and sends requests to Communications Service Provider (CSP);
- SPoC receives results back from CSP and returns results to Applicant; Applicant accesses the Web Viewer and downloads results; Original copy of application lodged with Legal Team.

3.11 Urgent Authorisations

3.11.1 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are not available.

3.12 Application Forms – Acquisition and Disclosure of Communications Data

3.12.1 Only the RIPA Forms listed below can be used by officers applying for RIPA authorisation.

- Application for a Section 22(4) RIPA Notice

- Notice under Section 22(4) RIPA requiring Communications Data to be Obtained and Disclosed

3.13 Duration of the Authorisation

3.13.1 A communications data notice remains valid for a **maximum of one month.**

3.13.2 Notices should not be permitted to expire, they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that all notices must be reviewed to decide whether to cancel or renew them.

3.14 Review of Authorisations

3.14.1 As referred to at 3.8.6, designated persons must make arrangements to periodically review any authorised RIPA activity. Officers carrying out RIPA activity, or external agencies engaged by the Council to carry out RIPA activity, must periodically review it and report back to the designated person if there is any doubt as to whether it should continue. Reviews should be recorded on the appropriate Home Office Form (see 3.13).

3.14.2 A copy of the Council's notice of review of an authorisation must be sent to the Monitoring Officer as soon as possible to enable the central record on RIPA to be authorised.

3.15 Renewal of Authorisations

3.15.1 If the designated person considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained. Renewed authorisations will normally be for a period one month in the case of a communications data authorisation or notice. Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation. The reasoning for seeking renewal of a communications data authorisation or RIPA notice should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

3.15.2 **All renewals will require an order of the Magistrates Court in accordance with the requirements in para 3.10 above.**

3.15.3 A copy of the Council's notice of renewal of an authorisation must be considered by the Monitoring Officer before it is made and all original copies lodged with the Legal Team together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

3.16 Cancellation of Authorisations

3.16.1 The person who granted or last renewed the authorisation must cancel it when they are satisfied that the communications data authorisation or notice no longer meets the criteria for authorisation. Cancellations must be made on the appropriate Home Office Form (see 8.6). In relation to a Section 22(4) notice to a CSP, the cancellation must be reported to the CSP by the designated person directly or by the SPoC on that person's behalf.

3.16.2 A copy of the Council's notice of cancellation of an authorisation must be sent to the Monitoring Officer within one week of the cancellation to enable the central record on RIPA to be updated.

3.17 What happens if the acquisition of communications data has unexpected results?

3.17.1 Those involved in the acquisition of communications data should inform the designated person if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

3.18 Records and Documentation

Departmental Records

3.18.1 Applications, renewals, cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

3.18.2 In relation to communications data, records must be held centrally by the SPoC. These records must be available for inspection by ICCP and retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions.

Central Record of Authorisations, Renewals, Reviews and Cancellations

3.18.3 A joint central record of access to communications data authorisations is maintained by the Monitoring Officer at the District Council Offices, Mill Lane, Wingerworth.

3.18.4 See paragraph 2.24 for more information on the central records, which also applies relation to covert surveillance and CHIS.

3.19 Communications data related to pending or future proceedings

3.19.1 Where the communications data acquired could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

3.19.2 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996 and on the Home Office website. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

3.19.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use RIPA to facilitate its use in other investigations.

3.19.4 Material obtained through acquisition of communications data containing personal information will be protected by GDPR and the Data Protection Act (DPA) and in addition to the considerations above must be used, stored and destroyed in compliance with the appropriate requirements of the GDPR/DPA and the Council's Data Protection, Information Security and Records Management Policies.

North East Derbyshire District Council

Standards Committee

28th February 2024

Annual Review of Whistleblowing Policy

Report of the Monitoring Officer

Classification**:** This report is public

Report By**:** **Sarah Sternberg, Assistant Director of Governance and Monitoring Officer.**

Contact Officer: **Sarah Sternberg, Assistant Director of Governance and Monitoring Officer.**

PURPOSE / SUMMARY

The Whistleblowing Policy should be reviewed annually and the number of confidential disclosures reported to Standards Committee. This was last done on the 6th December 2022.

A light touch review has been undertaken and is being reported to Members.

RECOMMENDATIONS

1. To approve the amended policy for including on the Council's website.

2. To note that no disclosures have been made under the policy in 2023.

IMPLICATIONS

Finance and Risk: **Yes☐** **No ☒**

Details:

On Behalf of the Section 151 Officer

Legal (including Data Protection): **Yes☒** **No ☐**

Details:

As in the report.

The Council is obliged to have arrangements in place.

On Behalf of the Solicitor to the Council

Staffing: Yes☐ No ☒
Details:

None

On behalf of the Head of Paid Service

DECISION INFORMATION

Decision Information	
Is the decision a Key Decision? A Key Decision is an executive decision which has a significant impact on two or more District wards or which results in income or expenditure to the Council above the following thresholds: **NEDDC:** **Revenue - £100,000 ☐ Capital - £250,000 ☐** ☒ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
District Wards Significantly Affected	None directly
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	Yes Details:

Links to Council Plan (NED) priorities, including Climate Change, Equalities, and Economics and Health implications.
Continually improve Council services to deliver excellence and value for money.

REPORT DETAILS

1 <u>Background</u> *(reasons for bringing the report)*

1.1 Whistleblowing is a report from an employee, member or other person about suspected wrongdoing within the organisation. The Public Interest Disclosure Act 1998 requires employers to refrain from dismissing workers

and employees or subjecting them to any other detriment because they have made a protected disclosure.

1.2 Whistleblowing policies should foster a climate of openness and transparency in which individuals in the workplace do not feel that they will be victimised, harassed or suffer any reprisals if they raise concerns about wrongdoing within the organisation. The Government expects all public bodies to have adequate whistleblowing procedures in place.

1.3 The Whistleblowing Policy was last reviewed in December 2022 when no substantive changes were recommended other than housekeeping amendments.

1.4 In accordance with the Whistleblowing Policy, the Monitoring Officer has overall responsibility for the maintenance and operation of the Policy, and will maintain a record of concerns raised and the outcomes. The Monitoring Officer is also required to report as necessary to Council on instances of Whistleblowing. There have been no instances to report for the 2023 calendar year.

2. Details of Proposal or Information

2.1 The Whistleblowing Policy has been reviewed to ensure that it remains fit for purpose and it is concluded that the existing version is satisfactory and up to date with current legislation and best practice. Some housekeeping changes have been made and a copy of the amended Policy is attached.

2.2 There are no instances of Whistleblowing to report to Members.

2.4 The policy, once approved, will be put on the Council's website and kept in HR.

3 Reasons for Recommendation

3.1 To ensure that the Whistleblowing Policy is up to date and regularly reviewed and considered by Members.

4 Alternative Options and Reasons for Rejection

4.1 There are no alternative options as the Policy needs regular review.

DOCUMENT INFORMATION

Appendix No	Title
1	Draft Whistleblowing Policy

Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet you must provide copies of the background papers)
None

North East Derbyshire District Council

Whistleblowing Policy

North East Derbyshire District Council

CONTROL SHEET FOR WHISTLEBLOWING POLICY

Policy Details	Comments/Confirmation (to be updated as the document progresses)
Policy title	Whistleblowing Policy
Current status –	Draft 2024 version, with housekeeping changes only.
Location of Policy –	HR
Member route for approval	Standards Committee
Cabinet Member (if applicable)	N/A
Equality Impact Assessment (approval date)	N/A
Partnership Involvement (if applicable)	N/A
Draft Policy for consideration	February 2024
Final Policy approval route (i.e. Executive/Council Committee)	Standards Committee
Date Policy approved	TBC

Date Policy due for review	Annually
Date Policy forwarded to be included on the Extranet and Internet.	

WHISTLEBLOWING POLICY

1. Introduction

1.1 Employees are often the first to realise that there may be something seriously wrong within a local authority. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the Council. They may also fear harassment or victimisation. In these circumstances employees may feel that it is easier to ignore the concern, rather than report what may just be a suspicion of malpractice.

1.2 The Council is committed to the highest possible standards of openness, probity and accountability. In line with that commitment the Council encourages employees, Members and others with serious concerns about any aspect of the Council's work to come forward and voice those concerns. It is recognised that certain cases will have to proceed on a confidential basis.

1.3 Whistleblowing is the term used when someone who works in or for an organisation raises a concern about a possible fraud, crime, danger or other serious risk that could threaten customers, colleagues, the public or the organisation's own reputation. For example instances of theft from the Council, accepting or offering a bribe, and failure by colleagues to adhere to Health & Safety directives could all be the subject of a Whistleblow.

1.4 This policy document makes it clear that concerns can be raised without fear of victimisation, subsequent discrimination or disadvantage. This Whistleblowing Policy is intended to encourage and enable employees to raise concerns within either Council in person, rather than overlooking a problem or using other methods to report concerns.

1.5 This policy applies to Council employees and other workers, including freelance staff, temporary and agency staff, trainers, volunteers, consultants, contractors, employees of another Local Authority with whom the Council has entered into joint working arrangements and Members.

1.6 This policy also applies to all employees in organisations who work in partnership with the Councils and suppliers who wish to raise a concern.

1.7 The Public Interest Disclosure Act 1998 protects Council employees who report concerns from subsequent harassment, victimisation and other unfair treatment. Potential informants should feel reassured that it is illegal for the Council to consider any action against them should their concerns not prove to be verifiable.

2. Aims and Scope of this Policy

2.1 This policy aims to:-

- encourage persons to feel confident in raising serious concerns that they may have about practices and procedures.

- provide avenues to raise those concerns and receive feedback on any action taken.

- allow persons to take the matter further if they are dissatisfied with the Council's response.

- reassure employees that they will be protected from possible reprisals or victimisation if they have made any disclosure.

2.2 Areas covered by the Whistleblowing Policy include:-

- criminal or other misconduct
- breaches of the Council's Standing Orders or Financial Regulations
- contravention of the Council's accepted standards, policies or procedures
- disclosures relating to miscarriages of justice
- health and safety risks
- damage to the environment
- unauthorised use of public funds
- fraud, bribery and corruption
- sexual, physical and/or verbal abuse of any person or group
- other unethical conduct
- the concealment of any of the above

2.3 Any concerns about any aspect of service provision or the conduct of officers or Elected Members of the Council, or others acting on behalf of the Council, can be reported under the Whistleblowing Policy. This may be about something that:-

- Makes you feel uncomfortable in terms of known standards, your experience or the standards you believe the Council subscribes to; or
- Is against the Council's Constitution and policies; or
- Falls below established standards of practice; or
- Amounts to improper conduct.

3. When this Policy may not be appropriate

3.1 This policy is not a substitute for the Council's other policies and procedures on such matters as personal grievances, bullying and harassment, health and safety, safeguarding issues (children and/or adults) complaints or complaints that Members have breached the Code of Conduct. It should also not be used to raise matters relating to an employee's own terms and conditions of service.

3.2 It is important to know the difference between a 'Whistleblow' and a 'grievance.' A Whistleblow has a public interest aspect to it, as it puts others at risk.

3.3 A grievance by contrast has no public interest factors, as it is a complaint about a particular employment situation. A grievance should be reported using the Grievance Policy, not this policy.

3.4 For example, a member of staff being formally interviewed on capability grounds, without previously having had any indication that their performance was not acceptable, may lead to a grievance complaint being made. Whilst a member of staff who observes colleagues sharing/selling confidential data to un-authorised others, should lead to a Whistleblow.

3.5 The policy is not to be used by members of the public to pursue complaints about services. These should be dealt with through the Council's Complaints Procedures.

3.6 This Policy is not to be used by members of the public to pursue complaints against Councillors' conduct. They should direct complaints in the first instance to the Monitoring Officer who will deal with their complaints under the Members Code of Conduct procedure.

4. Safeguards against Harassment or Victimisation

4.1 The Council recognises that the decision to report a concern can be a difficult one to make, not least because of the fear of reprisal from those responsible for the malpractice. However, the Council will not tolerate any form of harassment or victimisation and will take appropriate action to protect persons who have made a disclosure.

4.2 The Council is committed to good practice and high standards and endeavours to be supportive of persons who raise concerns under this Policy.

4.3 In all cases, the provisions of The Public Interest Disclosure 1998 (PIDA) will be adhered to.

4.4 The Enterprise & Regulatory Reform Act 2013 (ERRA) introduced a Public Interest test requirement on Whistleblowers. In order to receive the protection of PIDA, Whistleblowers will now have to show that they reasonably believe that the disclosure they are making is in the public Interest.

5. Confidentiality

5.1 All concerns will be treated in confidence and the identity of the person raising the concern will not be revealed without his or her consent (subject to any legal requirements or decisions). At the appropriate time, however, the person may be expected to come forward as a witness.

6. Anonymous Allegations

6.1 This policy encourages you to put your name to any allegation wherever possible and receive the protection of PIDA as anonymous complaints are likely to be difficult to deal with effectively.

6.2 Concerns expressed anonymously will be considered at the discretion of the Council. In exercising this discretion the factors to be taken into account would include:-

- The seriousness of the issues raised
- The credibility of the concern; and
- The likelihood of confirming the allegation from attributable sources.

7. Untrue Allegations & Legal Protection

7.1 If you are a Council employee, you are given legal protection by the Public Interest Disclosure Act 1998. You will qualify for this protection if you reasonably believe that the disclosure is in the public Interest.

7.2 If you make what is known as a “qualifying disclosure” under the 1998 Act to your employer or certain other persons/bodies, it will be unlawful for the Council to subject you to any detriment (such as denial of promotion or withdrawal of a training opportunity), or to dismiss you, because of the disclosure.

7.3 Qualifying disclosures are disclosures of information where a Council employee reasonably believes (and it is in the public interest) that one or more of the following matters is either happening, has taken place, or is likely to happen in the future.

- A criminal offence
- The breach of a legal obligation
- A miscarriage of justice
- A danger to the health and safety of any individual
- Damage to the environment
- Deliberate attempt to conceal any of the above.

7.4 Compensation may be awarded to you by an Employment Tribunal if the Council breaches the 1998 Act, following a successful claim for ‘detrimental treatment’.

8. How to raise a Concern under this Policy

8.1 Concerns may be raised normally in writing. Persons who wish to raise a concern should provide details of the nature of the concern or allegation in the following format:

- The background and history of the concern giving names, dates and places where possible.
- The reason why you are particularly concerned about the situation.
- Submit any relevant evidence or documentation.

8.2 The earlier you express the concern the easier it is to take action.

8.3 Although you are not expected to prove beyond reasonable doubt the truth of an allegation, you will need to demonstrate to the person contacted that there are reasonable grounds for your concern.

8.4 Employees may choose to be represented by a colleague or Trade Union representative.

Employees

8.5 Employees should normally raise concerns in the first instance with their Line Manager. Alternatively, dependent upon the nature, seriousness and sensitivity of the issues involved and the person suspected of malpractice you could approach;

- the Service Manager whom you feel would be the most appropriate
- Internal Audit
- the Head of Paid Service (responsible Officer for Safeguarding)
- the Monitoring Officer
- The Section 151 Officer

8.6 You may choose to contact a Prescribed Person. Prescribed persons, as prescribed under the Public Interest Disclosure Act 1998, are independent bodies or individuals that can be approached by whistleblowers where an approach to their employers would not be appropriate. Prescribed persons, which usually have an authoritative relationship with the whistleblowers' organisations, can be regulatory or legislative bodies, central government departments, arm's length bodies or charities and include all Members of Parliament. You may also contact the charity PROTECT. This is the new name for the "Public Concern at Work" charity. If you wish to remain anonymous you could contact this charity. The telephone numbers for this service is 020 7404 6609 and 020 3117 2550.

Other Persons (including Elected Members)

8.7 Other persons can contact any of the following officers of the Councils directly:

- the Service Manager whom you feel would be the most appropriate
- Internal Audit
- the Head of Paid Service (responsible Officer for safeguarding)
- the Monitoring Officer
- The Section 151 Officer

8.8 Officers of the Councils can be contacted in writing, by telephone or by going through one of the Contact Centres. You can contact the Council through your elected Councillor if this is preferable or more convenient.

8.9 You may also choose to contact a body external to the Council such as the External Auditor or the Police or a Prescribed Person.

9 How the Council will respond to a concern raised under this Policy

9.1 The Officer with whom the concern was initially raised will respond in writing within ten working days:

- acknowledging that the concern has been received

- indicating how it is proposed to deal with the matter
- stating whether any initial enquiries have been made
- supplying information on what support is available and stating whether further investigations will take place and if not, why not

9.2 Concerns raised under this Policy will be investigated by the investigating officer who will be appointed at the Council's discretion.

9.3 When conducting the investigation, the investigating officer may involve:-

- Internal Audit
- Legal & Governance Services
- Human Resources
- the Police (in some circumstances the Council will have no choice but to inform the Police if it believes a criminal offence has been committed and may do so without informing the whistle blower)
- an external auditor
- The Monitoring Officer
- The S 151 Officer
- The Head of Paid Service (responsible Officer for safeguarding)
- Any other person at the discretion of the investigating officer

9.4 The investigating officer should in the first instance inform any employee who is the subject of a Whistleblowing allegation of the allegation before a decision is taken as to what will happen with it. If the investigating officer determines that this would not be appropriate in the circumstances, then he should seek guidance from the Monitoring Officer who may advise not to inform the employee at this stage of the process.

9.5 The investigating officer will make initial enquiries to decide whether an investigation is appropriate and if so what form it should take having regard to the law and the public interest.

9.6 If the investigating officer decides that a disciplinary investigation is the appropriate course of action to take, he/she will advise Human Resources who will instruct an appropriate person to conduct the disciplinary investigation and ensure that the investigation is carried out in accordance with the Councils' Disciplinary Policy.

9.7 Some concerns may be resolved by agreed action without the need for investigation.

9.8 It may be necessary to take urgent action before any investigation is completed.

9.9 The Council will take steps to minimise any difficulties that persons may experience as a result of raising a concern. For instance, if he or she is required to give evidence in criminal or disciplinary proceedings the Council will arrange for advice to be given about the procedure (but not about what answers to give).

9.10 The Council accepts that persons need to be assured that the matter has been properly addressed. Subject to legal constraints, the Council will inform the Whistleblower of the progress and outcome of any investigation.

9.11 It is important for persons to understand that making a Whistleblowing allegation doesn't give them anonymity, but does give them protection from harassment or victimisation.

10 The Responsible Officer

10.1 The Monitoring Officer has overall responsibility for the maintenance and operation of this Policy, and will maintain a record of concerns raised and the outcomes. This record will be in a form which does not compromise confidentiality and substantially in the form attached.

10.2 The Monitoring Officer will report as necessary to the Council.

10.3 The Investigating Officer must inform the Monitoring Officer of the receipt of a concern raised under this Policy, how they intend to deal with it and how the matter was concluded.

11. How the Matter Can Be Taken Further

11.1 This Policy is intended to provide a process within the Council, through which appropriate persons may raise concerns. If at the conclusion of this process the person is not satisfied with any action taken or feels that the action taken is inappropriate, the following are suggested as further referral points:

- the Council's external auditor
- Your Trade Union
- Your local Citizens Advice Bureau
- Relevant professional body or regulatory organisation
- A relevant voluntary organisation
- The Police
- Your Solicitor
- The Audit Commission

11.2 Advice should be taken before making an external disclosure and the internal procedure should normally have been followed first.

11.3 The Council would not normally expect Whistleblowers to make disclosures to the press.

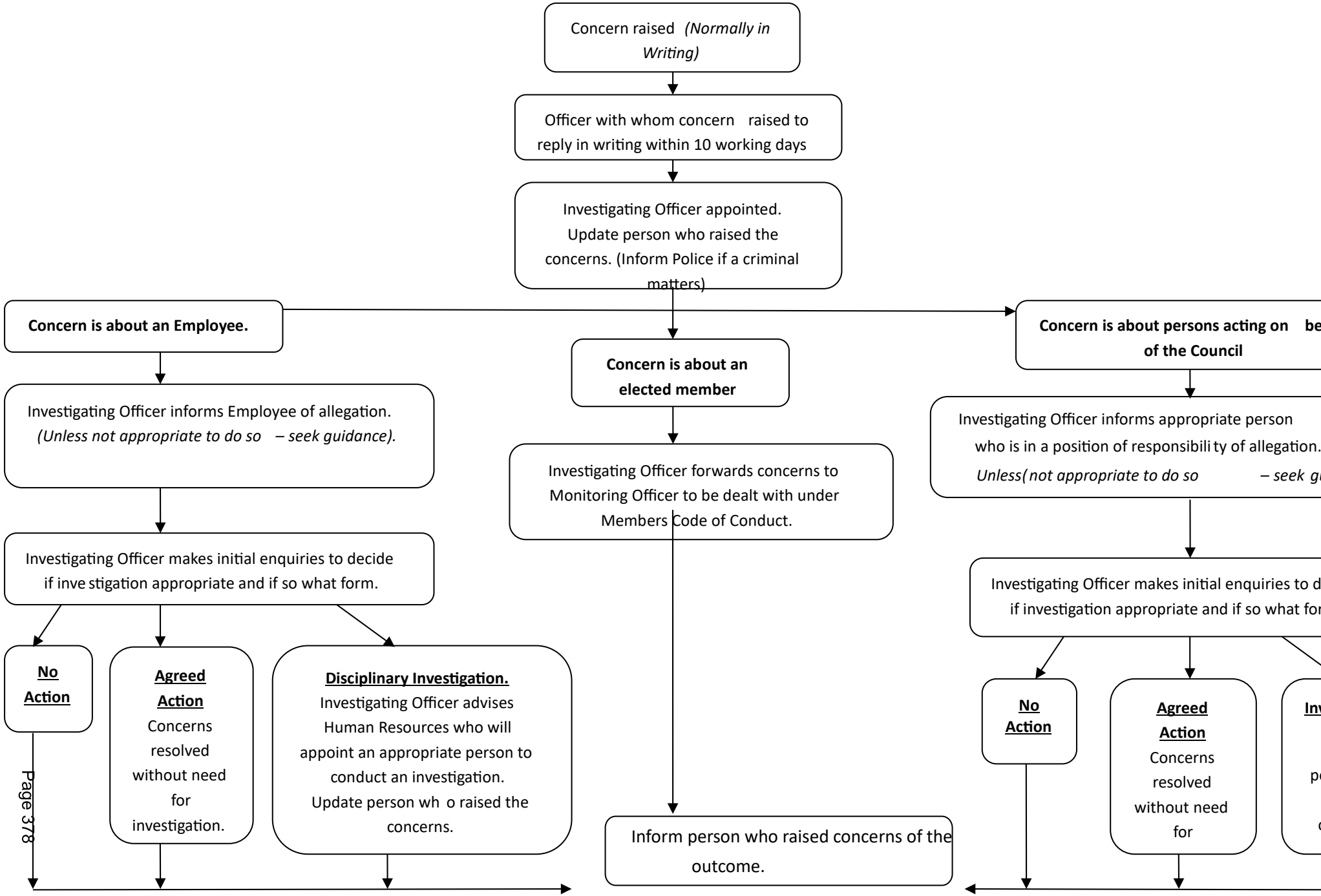
12. Whistleblowing Register

12.1 The Monitoring Officer in accordance with the Whistleblowing Policy of North East Derbyshire District Council has overall responsibility for the maintenance and operation of this Policy, and will maintain a record of concerns raised and the

outcomes. This record will be in a form which does not compromise confidentiality and substantially in the form below.

Number	Council	Details	Outcome
1/20xx			

WHISTLEBLOWING POLICY FLOWCHART


Concern raised (Normally in Writing)
Officer with whom concern raised to reply in writing within 10 working days
Investigating Officer appointed. Update person who raised the concerns. (Inform Police if a criminal matters)
Concern is about an Employee.
Concern is about an elected member
Concern is about persons acting on be of the Council
Investigating Officer informs Employee of allegation. (Unless not appropriate to do so – seek guidance).
Investigating Officer forwards concerns to Monitoring Officer to be dealt with under Members Code of Conduct.
Investigating Officer informs appropriate person who is in a position of responsibili ty of allegation. Unless(not appropriate to do so – seek g
Investigating Officer makes initial enquiries to decide if inve stigation appropriate and if so what form.
Investigating Officer makes initial enquiries to d if investigation appropriate and if so what for
No Action
Agreed Action Concerns resolved without need for investigation.
Disciplinary Investigation. Investigating Officer advises Human Resources who will appoint an appropriate person to conduct an investigation. Update person wh o raised the concerns.
Inform person who raised concerns of the outcome.
No Action
Agreed Action Concerns resolved without need for
Inv
pe

North East Derbyshire District Council

Standards Committee

28 February 2024

Complaint Update Report

Report of the Assistant Director of Governance and Monitoring Officer

Classification**:** This report is public.

Report By**:** Sarah Sternberg, Assistant Director of Governance and Monitoring Officer, sarah.sternberg@ne-derbyshire.gov.uk

Contact Officer: Asher Bond, Governance Officer – asher.bond@ne-derbyshire.gov.uk

---

PURPOSE / SUMMARY

To provide Standards Committee with an update on the number of complaints that have been received and what action has been taken on these.

RECOMMENDATIONS

That the Standards Committee notes the complaints update.

IMPLICATIONS

Finance and Risk: **Yes☐** **No ☒**
Details:

On Behalf of the Section 151 Officer

Legal (including Data Protection): **Yes☐** **No ☒**
Details:

On Behalf of the Solicitor to the Council

Staffing: **Yes☐** **No ☒**
Details:

On behalf of the Head of Paid Service

DECISION INFORMATION

Decision Information	
Is the decision a Key Decision? A Key Decision is an executive decision which has a significant impact on two or more District wards or which results in income or expenditure to the Council above the following thresholds: **NEDDC:** **Revenue - £100,000 ☐ Capital - £250,000 ☐** ☒ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
District Wards Significantly Affected	None
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	No

Links to Council Plan (NED) priorities, including Climate Change, Equalities, and Economics and Health implications.

REPORT DETAILS

1 <u>Background</u> *(reasons for bringing the report)*

1.1 Under Section 28 (6) and (7) of the Localism Act 2011, the Council must have in place “arrangements” under which allegations that a member or co-opted member of the Council or parish or town council within its area has failed to comply with that Authority’s Code of Conduct can be investigation and decisions made on such allegations.

1.2 The Council has adopted a Code of Conduct for Members. Each parish or town council is also required to adopt a Code of Conduct.

1.3 The Monitoring Officer is a senior officer of the Authority who has the statutory responsibility for administering the system in respect of complaints of member misconduct.

1.4 Standards Committee is to receive regular reports from the Monitoring Officer on the number of complaints against members, how they are progressing, what decisions have been made and what action taken.

2. Details of Proposal or Information

2.1 Since the last update was brought to Committee in September, four new complaints have been opened and seven complaints have been closed. There are currently a total of six ongoing complaints.

2.2 Of the complaints that were closed, two proceeded to investigation.

The investigation concluded that in one case it would no longer be in the public interest to continue to pursue the complaint.

The investigation concluded that in one case, there had been a breach of the Code of Conduct. However, the investigation revealed more underlying systemic concerns about the Council which should be addressed as a priority. As such, a number of steps were recommended to the Parish Council, these included compulsory training for all Members on the Code of Conduct and Standing Orders with a particular focus on behaviours, the conduct of business and decision-making processes.

2.3 Two complaints were closed as there was not enough evidence provided to suggest that a breach had taken place or that the Member was acting in their capacity as a Councillor at the time of the alleged incidents.

One complaint was closed because the Member had apologised for their behaviour during the meeting in question.

One complaint was closed because there was no evidence that the Member was lying or that they had expressed their opinion in an objectionable way.

One complaint was closed because there was no evidence that the Member was dishonest or misleading during the meeting in question.

3 Reasons for Recommendation

3.1 Under the North East Derbyshire District Council's Constitution It is a function of the Standards Committee to receive regular update reports from the Monitoring Officer on the number of complaints received against members, how they are progressing, what decisions have been made and what actions taken.

4 Alternative Options and Reasons for Rejection

4.1 There are no alternative options to consider as part of this report.

DOCUMENT INFORMATION

Appendix No	Title
1	Complaint Update
Background Papers (These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Cabinet you must provide copies of the background papers)	

APPENDIX 1 - NEDDC COMPLAINTS MADE AGAINST MEMBERS – QUARTERLY UPDATE

List of Cases which do not proceed to investigation

DATE OF RECEIPT	PART OF CODE OF CONDUCT ALLEGED TO HAVE BEEN BREACHED	NAME OF COUNCIL	WHETHER A POTENTIAL BREACH WAS FOUND	REASONS FOR DECISION
10/02/23 **02/2023**	Treating all persons fairly and with respect.	North East Derbyshire District Council	**No**	There was not enough evidence to suggest that the Member was acting their capacity as a Councillor at the time of the alleged incidents.
21.04.23 **07/2023**	Bullying and harassment Treating all persons fairly and with respect	Eckington Parish Council	**No**	There was not enough evidence to suggest that a breach had taken place or that the Member was acting in their capacity as a Councillor at the time of the alleged incidents.
17/07/23 **12/2023**	Valuing my colleagues and staff and engaging with them in an appropriate manner and one that underpins the mutual respect between us that is essential to good local government. Always treating people with respect, including the organisations and public I	Shirland and Higham Parish Council	**No**	The Member apologised for their behaviour during the meeting in question.

	engage with and those I work alongside. Providing leadership through behaving in accordance with these principles when championing the interests of the community, with other organisations, as well as within the Council.			
31/07/23 **14/2023**	Honesty, objectivity and not using my position as a Councillor improperly to the advantage or disadvantage of myself or anyone else.	North East Derbyshire District Council	**No**	There was no evidence that the Member was lying or that they expressed their opinion in an objectionable way.
26/07/23 **15/2023**	Honesty and objectivity.	North East Derbyshire District Council	**No**	There was no evidence that the Member was dishonest or misleading during the meeting in question.

Date	Agenda items
27th July 23	• Code of Corporate Governance • Scrutiny Committees Terms of Reference • LGA guidance on complaints processing/Flow Chart • Planning Committee number of speakers – kick off debate • Parish Cllrs representatives selection process • Scrutiny Committee Terms of Reference
27th September 23	• Progress on Planning Committee speakers issue • Annual Letter from the Local Government Ombudsman • The 2023-24 Review of the Constitution
15th November 23	• Choice of PC representatives as per report • Annual Parish Conference
28th February 24	• Social Media guidance for Members – policy? • RIPA Policy Review • Whistleblowing Policy Review
17th April 24	• Annual report of Standards Committee • Annual report of the Independent Persons • Final changes to the Constitution • Review of Members' Attendance at Training Events • Holding Meetings at Alternative Venues • Review Members complaints Process and Complaints Procedure including flow charts • Standards Committee training proposals for District Councillors – Kick off consideration • Options for Parish Cllrs training • Visits to other Standards Committees?