Public Document Pack

North East Derbyshire District Council

Contact: Torin Fuller - Governance Officer
Tel: 01246 217375
Email: torin.fuller@ne-derbyshire.gov.uk

Date: Tuesday, 21 April 2026

To: **Members of the Standards Committee**

Please attend a meeting of the Standards Committee to be held on Wednesday, 29 April 2026, at 10.00 am in Executive Meeting Room at the 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 P Antcliff Councillor P Kerry Councillor K Rouse	Councillor H Wetherall (Vice-Chair) Councillor C Cupit Councillor F Petersen

Any substitutions must be notified to the Governance Manager in advance by midday the working day before the meeting.

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 - 7)

To approve as a correct record and the Chair to sign the Minutes of the Standards Committee held on 25 February 2026.

4 Review of the Constitution (Pages 8 - 12)

5 Review of Members' Attendance at Training Events (Pages 13 - 16)

6 RIPA Policy Annual Report (Pages 17 - 64)

7 Whistleblowing Policy Annual Report (Pages 65 - 85)

8 Planning Site Visit Protocol (To Follow)

9 Social Media Guidance for Councillors - Appendix 5 of the Constitution (Pages 86 - 99)

10 Disciplinary Procedure for Statutory Officers (Pages 100 - 107)

11 Member Officer Relations Protocol (To Follow)

12 Meeting Times

13 Work Programme (Page 108)

14 Urgent Business

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 2013 Mill Lane, Wingerworth, S42 6NG

STANDARDS COMMITTEE

MINUTES OF MEETING HELD ON WEDNESDAY, 25 FEBRUARY 2026

Present:

Councillor Kevin Gillott (Chair) (in the Chair)
Councillor Helen Wetherall (Vice-Chair)

Councillor Pat Antcliff
Councillor Fran Petersen
Councillor Pat Kerry
Councillor Kathy Rouse

Also Present:

A Smith	Legal Services Manager and Deputy Monitoring Officer
A Bryan	Governance Manager
T Fuller	Senior Governance Officer

STA/30/25-26 **Apologies for Absence**

Apologies for absence were received from Councillor C Cupit.

STA/31/25-26 **Declarations of Interest**

There were no declarations of interest.

STA/32/25-26 **Minutes of Last Meeting**

RESOLVED –

That the minutes of the meeting of the meeting held on 12 December 2025 be approved as a correct record and signed by the Chair.

STA/33/25-26 **Member Officer Protocol**

Committee considered a report which presented the draft revised Member Officer Relations Protocol. The report highlighted that the Local Government Association (LGA) advised a much more inclusive review when creating and reviewing such protocols. Therefore, Members were being asked to consider how to move this forward, as well as considering the immediate changes to the document.

Committee discussed the report. Some Members suggested that a substantive review may not be appropriate in light of Local Government Reorganisation (LGR). Some Members suggested that a more direct approach may be needed when tackling recent issues, regarding Member – Officer relations. The Committee discussed how to appraise Members of the changes to the protocol, and it was agreed that the final protocol would be sent to the respective Group Leaders.

RESOLVED –

1. That the Rules for Councillor – Officer Relations be renamed the Member

Officer Relations Protocol to align it with the LGA guidance.

2. That Members commented on and approved the amended version for inclusion in the Constitution for 2026.

3. That the Monitoring Officer and the Governance Manager bring a report to the next meeting in relation to the issues raised by the LGA guidance on Member Officer Relations Protocol.

STA/34/25-26 **Annual Gifts and Hospitality Report**

Committee considered a report which advised of the details of all entries in the Council's Gifts and Hospitality Register in respect of offers of gifts and hospitality made to Members and officers of the Council during the period January 2025 to December 2025.

Committee discussed the report. Some Members referenced the fact that there were few gifts, and they were small in value.

RESOLVED –

That the contents of the annual report in respect of offers of gifts and hospitality made to Members and officers for the period January 2025 to December 2025, be noted.

STA/35/25-26 **Code of Conduct - Recent Cases Update**

Committee considered a report which updated Members with specific recent Code of Conduct cases. The report included details on each case and the result of each investigation.

Committee discussed the report. Some Members suggested that, in relation to the WhatsApp case, it should be made clear that people need to be careful even when using a personal phone. It was agreed that the cases would be emailed to the Group Leaders.

RESOLVED –

That the report be noted.

STA/36/25-26 **Review of the Constitution**

Committee considered a report which progressed the annual process of reviewing the Constitution. The report proposed amendments relating to Advisory Bodies, Community Governance Reviews, Questions by Councillors and Council Motions.

Committee discussed the report. Some Members had queries relating to advisory bodies. It was clarified that there was no advisory body relating to LGR and it was agreed that appropriate wording would be added to allow the Monitoring Officer to add and take out advisory bodies where necessary. Some Members suggested that the amendments relating to Questions by Councillors and Council Motions would create some uncertainty, but it was felt that the changes were sensible and

any interpretation could be done by the Monitoring Officer.

RESOLVED –

That the proposed changes be agreed and recommended to Council for inclusion in the Constitution.

STA/ 37/25-26 **Sub-Committee Hearing Procedure**

Committee considered a report which sought approval to establish a Standards Sub-Committee to consider and determine allegations that a Member had breached the Code of Conduct.

Committee considered the report. It was felt that the procedure set out was a fair one. Members discussed who would sit on the Sub-Committee, it was suggested that the Sub-Committee comprise of one Labour, one Conservative and one Independent Member where possible.

RESOLVED –

1. That a Standards Sub-Committee be established.

2. That the hearing procedure, to be followed by the Standards Sub-Committee when conducting a hearing, be approved.

STA/ 38/25-26 **Complaints Update**

The Legal Services Manager and Deputy Monitoring Officer provided an update on the number of complaints that had been received against Councillors. Members heard that there were 9 ongoing complaints in total, the majority of which were NEDDC Councillors, and the reasons for the complaints were clarified.

Committee discussed the update. Some Members queried whether Councillor's social media channels were monitored. Members heard that officers were looking into the options available where a Councillors post was of a defamatory nature against the Council. It was highlighted that any post that raised safeguarding issues needed reporting.

RESOLVED –

That the update be noted.

STA/ 39/25-26 **Work Programme**

The Committee considered its work programme for the remainer of the 2025/26 Municipal Year.

RESOLVED – that the work programme be noted.

STA/ 40/2 **Urgent Business**

5-26 None.

Proposed changes to the Constitution. **Changes in red.** Page references are to the Constitution pages.		
Provision of the Constitution	Proposed change and reasons	Final version proposed
Planning Committee Terms of Reference, paragraph g	Under a strict interpretation of paragraph g in the Planning Committee Terms of Reference, a consultant isn't caught by the requirement for an application in the circumstances listed, to go to Committee. in the same circumstances for a Council Officer, the application has to be determined by Planning Committee. This ensures openness and transparency when dealing with such applications.	(g) If a serving Councillor, senior officer or senior manager of the Council (Team Manager and above), Planning Officer or other Planning team member (including a consultant employed to carry out the role of a Planning Officer) advising or determining on planning applications, submits an application to the Authority for himself/herself or on behalf of any other person, or are the Partner or Relative of the same who submits their own application, they will inform both the Planning Manager and the Authority's Monitoring Officer and not take part in processing or determining the Application.
	In the same paragraph it is not clear that close personal friends are included as well as relatives.	Add to the end: For the avoidance of doubt the reference to "person" in this paragraph includes any relative, friend or close associate.
Council Procedure Rules, 12.7 Alteration of Motion		12.7 Alteration of Motion (a) A Councillor may alter a motion of which he or she has given notice with the consent of the meeting. The meeting's consent will be signified without discussion. "Friendly amendments" will be

		dealt with in this way, where the motion proposer agrees the proposed change.
Council Procedure Rules 9. Questions by Cllrs	There are some clarifications of questions which need to take place but currently there is no formal provision for the Monitoring Officer to reject them. For example, it is the case that on some occasions, questions outline facts which are incorrect. Currently there is negotiation between the Monitoring Officer and the Questioner to amend the facts. Should the Questioner be unwilling to amend, there is no direct reason for rejection of the question, unless the contents are defamatory, frivolous or offensive. In circumstances where the factual inaccuracies are significantly misleading this is not helpful to the debate or public perceptions of the Council. One way to deal with this is to add an additional power to paragraph 9.4 for the Monitoring Officer to reject a question in these circumstances.	Proposed additional paragraph 9.4 (i): (i) Where the text of the question contains substantially incorrect factual statements and the questioner refuses to amend the text of the question.
Council Procedure Rules 10. Motions – on Notice.	The same issue arises with motions proposed on notice – that the contents of the motion are substantially factually incorrect. This has the potential to be more damaging as Council is actually taking a decision on a motion. Again the system relies on the proposer of the motion	Proposed additional paragraph 10.2 Scope (j): (j) Where the text of the motion contains substantially incorrect factual statements and the proposer refuses to amend the text of the motion.

	agreeing to make changes to the wording of the motion. One way to deal with this is to add an additional power to paragraph 10.2 for the Monitoring Officer to reject a motion in these circumstances.	
	Where a motion seeks to change or make a Cabinet decision, it should not be possible for the motion to proceed. There is always an opportunity for the Monitoring Officer to discuss this with the motion proposer and seek a compromise. However if a motion proposer should refuse to amend the motion there is only the provision that allows the HOPS to advise the Chair that it is illegal. A clear statement that Council cannot make decisions that are within the Cabinet's functions could cover this. This would still allow debate by Council on whether and in what terms to refer a matter to Cabinet.	Add the following statement to 10.2 Scope: The Monitoring Officer will reject any motion which recommends the Council to make a decision in relation to a Cabinet function or to change a Cabinet decision. Such a motion will be referred to Cabinet for consideration.
11 Motions and amendments without notice.	Where the motion is complex – such as when an alternative budget is proposed – a response will need to be worked through and considered financially and legally in advance of the Council Meeting. This	Add after 10.6: 10.6 <u>Alternative Budget proposal</u> Prior to moving a motion or amendment in Council proposing an alternative budget to the

	should not therefore be a motion which is put forward without notice.	proposals of the Cabinet, a Cllr must in advance of the meeting seek the views of the Section 151 Officer. A failure to do so will result in the motion being rejected by the Chair. The motion must contain sufficient detail within it to justify the proposal. The Chair will take the advice of the Statutory Officers in determining this.
Appendix to the Constitution Two – Members' Travel and Subsistence Policy.	There is no requirement for Cllrs to submit their travel and subsistence claims within a specified time frame. Officers' claims should be submitted monthly and are subject to approval by the Section 151 Officer if claimed outside 3 months. There is therefore a decision to be made as to whether claims should be submitted by Members within 3 months of the claim arising.	Add in an extra sentence as follows: Members will submit claims within 3 months of the claim arising. All claims for a particular financial year are to be submitted within one month of 31 March.
Council Procedure Rules 10 Motions - on Notice	Currently there is no requirement for a Councillor proposing a motion to inform the Council who will be seconding the motion. Some Proposers do include this information. Some councils require that a motion is submitted by 2 Councillors – presumably the mover and seconder. This would give a degree of certainty as to what would be	10.1 Motions - on Notice Change the requirement to the motion being signed by two Councillors, so that it reads: Except for motions which can be moved without notice under Rule 11, written notice of every motion, signed by the proposed mover and seconder of the motion ~~at least one Councillor~~, must be delivered to the Monitoring Officer not later than midday on the day twelve clear working days

	moved and seconded at Council and prevents speculation on the day. Accordingly it is proposed to add this requirement to the Rules.	before the date of the meeting. These will be published on the Council's web site. There is a limit of one motion, per Councillor ~~Member~~, per meeting. Details of motions submitted by Councillors on notice will be circulated to the Cabinet immediately after the deadline has passed.
Changes to EAC	To ensure the full process is in place to deal with employment matters relating to the Statutory Officers.	This is on another report to Standards Committee.

North East Derbyshire District Council

Standards Committee

29 April 2026

Member Training Attendance 2025/26

Report of the Governance Manager

Classification: This report is public

Report By**:** Amy Bryan, Governance Manager

Contact Officer: Amy Bryan, Governance Manager

PURPOSE / SUMMARY

This report summarises attendance by Councillors at recent training sessions.

RECOMMENDATIONS

1. That the information on Member training attendances be noted.

IMPLICATIONS

Finance and Risk: **Yes☐** **No ☒**

Details:

On Behalf of the Section 151 Officer

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

Details: Essential training to cover the legal obligations and responsibilities of Members and the Council is included in the member development programme as part of induction and with regular refreshers. Subjects such as data protection, safeguarding, code of conduct will be addressed regularly, with committee specific training on an annual basis or as needed.

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 - £125,000 ☐ Capital - £310,000 ☐** ☒ *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
Equality Impact Assessment (EIA) details:	
Stage 1 screening undertaken • Completed EIA stage 1 to be appended if not required to do a stage 2	Not applicable. This report is for information only.
Stage 2 full assessment undertaken • Completed EIA stage 2 needs to be appended to the report	No, not applicable
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	Details:

Links to Council Plan priorities; • **A great place that cares for the environment** • **A great place to live well** • **A great place to work** • **A great place to access good public services**
Indirectly affects all the above.

REPORT DETAILS

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

1.1 Within the Terms of Reference of the Standards Committee is to: 'Oversee Member Training, (including the attendance of Members at courses), in relation to matters affecting their conduct and probity including relevant information provided to newly elected District Councillors.

1.2 The information in this report is set out for the Committee to monitor and oversee member training.

2. Details of Proposal or Information

2.1 The following training has been held during 2025/26:

Planning Committee Training – 25 June 2025
This training was aimed at those who had not completed any planning training, but all Planning Committee Members and Subs were invited to attend.
This session was delivered in person with the option to join on Teams.
All Planning Committee Members and named substitutes were invited and 11 Councillors attended.

Licensing Committee Training – 16 September 2025
This training provided an overview of the Licensing Service and aim to help Members understand their role and responsibilities as a Member of the Licensing Committee and provide guidance on good decision-making.
This session was delivered in person with the option to join on Teams.
All Licensing Committee Members were invited to attend and 6 Councillors attended.

2.2 For the mid-term induction refresh, officers have produced training videos which have been made available to Members. The following training videos have been made available:

- Emergency Planning
- Safeguarding
- Risk
- Finance
- Equality & Inclusion
- Community Safety
- Understanding Executive Decision Making
- Freedom of Information & Data Protection

Members were asked to confirm once they had watched the training videos so their training records could be updated.

So far, four Councillors have confirmed they have watched some or all of the training videos.

2.3 One member attended an externally run course – Chairing Skills for Members on 18 June 2025 run by East Midlands Councils.

2.4 Since November 2024, Councillors have had access to Me Learning, which is the Council's online learning platform. All Councillors received an email in November 2024 which invited them to set up an account on the platform. Councillors who are signed up then have access to the following nine courses:

- Information & Cyber Security
- NEDDC Safeguarding Awareness
- Freedom of Information
- GDPR / Data Protection
- Fire Safety Awareness
- Health & Safety in the Workplace
- NEDDC Mental Health Awareness
- Equality & Diversity
- Safeguarding against Radicalisation – Prevent Duty

Councillors were asked to complete the courses by 6 May 2025.

2.5 In January 2026 Councillors were sent a reminder about the training platform.

2.6 Twelve Councillors have so far set up an account on the software.

Other Training

2.7 Some Councillors have indicated that they have participated in similar training through other positions and have requested recognition to avoid repeating or undertaking training at a level below what is required for their other role(s). In response, if a Councillor provides details of previous training, including the provider and completion dates, this information will be recorded in the Councillor's official training record.

3 Reasons for Recommendation

3.1 To enable the Committee to carry out its role in monitoring member training.

4 Alternative Options and Reasons for Rejection

4.1 There are no alternative options as this report is for information only.

DOCUMENT INFORMATION

Appendix No	Title
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

Standards Committee

29th April 2026

Annual Review of RIPA Policy 2026

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

To report the outcome of the annual review of the RIPA Policy and Procedure.

RECOMMENDATIONS

1. That subject to Members' comments and relevant officers' comments, the RIPA policy is approved.

2. That delegated authority is given to the Assistant Director of Governance to amend the Policy following any comments received from Members or Officers.

IMPLICATIONS

Finance and Risk: **Yes☐** **No ☒**

Details:

On Behalf of the Section 151 Officer

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

Details:

It is a requirement to have such a Policy and the Register that goes with it and to review these annually. However like many Councils, this Council hasn't used the procedure for many years.

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 - £125,000 ☐ Capital - £310,000 ☐** ☒ *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
Equality Impact Assessment (EIA) details:	
Stage 1 screening undertaken • Completed EIA stage 1 to be appended if not required to do a stage 2	Yes, for previous review.
Stage 2 full assessment undertaken • Completed EIA stage 2 needs to be appended to the report	No, not applicable
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	Yes Details: Standards Committee

Links to Council Plan priorities; • **A great place that cares for the environment** • **A great place to live well** • **A great place to work** • **A great place to access good public services**
Indirectly all.

REPORT DETAILS

1 Background *(reasons for bringing the report)*

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) and amending legislation covers the public sector's use of directed covert surveillance and Covert Human Intelligence Source (CHIS). It also covers access to a limited amount of communications data. This latter has never been used by this Council.

1.2 The only purpose for which the powers can be used by a Council are for the prevention or detection of crime where the sanction on conviction would be greater than 6 months. It is not relevant to any kind of overt surveillance or to anything done in relation to administrative/private matters such as employment matters.

1.3 The policy was last reviewed in 2025 and an annual review is good practice.

1.4 The guidance on the use of social media in investigations is now included within the Policy itself.

2. Details of Proposal or Information

2.1 Changes made to the policy reflect changes in legislation and oversight. There are no fundamental changes.

2.2 Members may recall that online training was being produced in addition to the two yearly in person training. This is now at an advanced stage and we are waiting for the final version.

2.3 in relation to the use of social media in investigations, there is guidance within the policy itself together with forms to monitor its use. This is to aid managers in ensuring that social media use does not go beyond the acceptable and become something for which a RIPA authorisation is required. In addition to this, relevant managers have been asked to confirm for the year 2025/6 that they have monitored its use and no use has required a RIPA authorisation. I have had confirmation from Community Safety and await a response from Environmental Health and Planning.

3 Reasons for Recommendation

3.1 To ensure there is an up to date policy and procedures in place, should the Council wish to use these investigative tools.

4 Alternative Options and Reasons for Rejection

4.1 There is no alternative to reviewing the Policy.

DOCUMENT INFORMATION

Appendix No	Title
1	The draft RIPA Policy 2026

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

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

Section: Introduction

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	2026 version
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	March 2026
Partnership involvement (if applicable)	N/A
Final policy approval route i.e. Executive/ Council /Planning Committee	Standards Committee
Date policy approved	April 2026
Date policy due for review (maximum three years)	April 2027
Date policy forwarded to be included on Intranet and Internet if applicable to the public	Following April 2026 Standards Committee.

Contents

Section: Introduction

Abbreviations

AOs	Authorising Officers who are the Chief Executive Officer 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 on Human Rights
HRA	Human Rights Act 1998
IPCO	Investigatory Powers Commissioner's Office
NAFN	The National Anti Fraud Network
OCDA	The Office for Communications Data Authorisations
PFA	Protection of Freedoms Act 2012
IPA	Investigatory Powers Act 2016
RIPA	Regulation of Investigatory Powers Act 2000
SPoCs	Single Points of Contact for Acquisition and Disclosure of Communications Data
SRO	Senior Responsible Officer. This is the Assistant Director of Governance and Monitoring Officer.

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 Deputy Monitoring Officer .</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 Human Rights.

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** p**roportionate**

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:-

- Home Office Statutory Codes of Practice on the Gov.uk website.
- 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;
- Appointing Designated Persons;
- Maintaining a central record for all RIPA authorisations;
- Arranging training for individuals appointed as Authorising Officers and Designated Persons,
- Arranging training for individuals who would seek RIPA authorisations 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 or Deputy 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 publicly 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 Policy and Procedure. 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 publicly available; and
- Information is stored for an investigation.

1.4.4 The Social Media guidance includes details as to how access to social media should be monitored to ensure compliance.

1.4.5 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 Training on the Me Learning platform will become available during 2026/27.

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

1.5.5 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 or Deputy 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 by contacting the Monitoring Officer.

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 Commissioner 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 9.29 of the Home Office Covert Surveillance and Property Interference Code of Practice.

2.7.7 **Confidential journalistic material** is described at paragraph 9.36 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.

Under the 2000 Act, 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.

and if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. Guidance can be obtained from the Home Office "Covert Human Intelligence Sources code of practice".

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 the 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 sets 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. For more details please refer to the Council's "Use of Overt Surveillance Systems Policy".

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 2.14 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (2.20 – 2.23 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:
Chief Executive Officer and 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 2.12.4) 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 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 to 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 2.21), prior to the 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 For arrangements for submitting applications to the Magistrates, please contact Legal Services.

2.16.3 The Magistrates 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 approving 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.

2.18 Urgent Authorisations

2.18.1 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.

2.19 Application Forms

2.19.1 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

2.20 Duration of the Authorisation

2.20.1 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 months if a juvenile CHIS is issued);

2.20.2 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 <u>all</u> authorisations must be reviewed to decide whether to cancel or renew them.

2.21 Review of Authorisations

2.21.1 As referred to at 2.15.1 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 2.19.1).

2.21.2 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.

2.22 Renewal of Authorisations

2.22.1 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 2.14 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 2.19).

2.22.2 All renewals will require an order of the Magistrates Court in accordance with the requirements in para 2.17 above.

2.22.3 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.

2.23 Cancellation of Authorisations

2.23.1 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 2.19).

2.23.2 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.

2.24 What happens if the surveillance has unexpected results?

2.24.1 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.

2.25 Records and Documentation

Departmental Records

2.25.1 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

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

2.25.3 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 2.16) send notification of every renewal, cancellation and review on the Council's notification forms (see 2.19 – 2.22).

2.25.4 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.

2.26 Surveillance products

2.26.1 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.

2.26.2 Particular attention is drawn to the requirements of the Codes of Practice issued under the Criminal Procedure and Investigations Act 1996 by the Home Office and on the Home Office website. These require 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.

2.26.3 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.

2.26.4 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.

2.26.5 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.

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. Currently this Authority has not used these powers.

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

3.2 Communication Service Providers ("CSPs")

3.2.1 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.

3.3 Types of Communications Data

3.3.1 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:-

3.3.2 <u>Service Use Information</u>

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.

3.3.3 <u>Subscriber information</u>

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.

3.3.4 Traffic Information

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.**

3.4 Use of Communications Data

3.4.1 The Council will only authorise the acquisition of service use and entity information. Under no circumstances will the Council obtain traffic data or intercept communications data under RIPA as they are not empowered to do so.

3.4.2 Communications data is governed by the Regulation of Investigatory Powers 2000, (RIPA) the Investigatory Powers Act 2016 (IPA) and the Data Retention Acquisition Regulations 2018. These regulations introduced a higher threshold to be able to obtain communications data. Guidance on this is set out in the Home Office Communications Data Code of Practice 2025. A request for a RIPA authorisation or notice will be scrutinised by a single point of contact (a 'SPoC'). Local Authorities are not able to intercept communications data. Where communications data is required then responsibility for its acquisition rests with the Office for Communications Data Authorisation (OCDA). National Anti-Fraud Network (NAFN) provide the SPoC service for Local Authorities and any application to the OCDA must be submitted through the NAFN with whom this Council has an agreement. Where consideration is being given to obtaining communications data, in addition to contacting the Monitoring Officer, the guidance from the NAFN should be obtained from the Section 151 Officer or the Deputy Section 151 Officer and used in connection with the application.

3.4.3 NAFN have issued guidance which must be followed when considering any application. This guidance can be obtained from the NAFN website. Where consideration is being given to obtaining communications data, in addition to contacting the Monitoring Officer, the guidance from the NAFN should be obtained from the Section 151 Officer or the Deputy Section 151 Officer and used in connection with the application.

3.4.3 The Council must keep records of all decisions and outcomes from the OCDA as these records are not kept centrally. These will be kept on the RIPA Register 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.

3.6 Urgent Authorisations

3.6.1 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.

3.7 Central Record of Authorisations, Renewals, Reviews and Cancellations

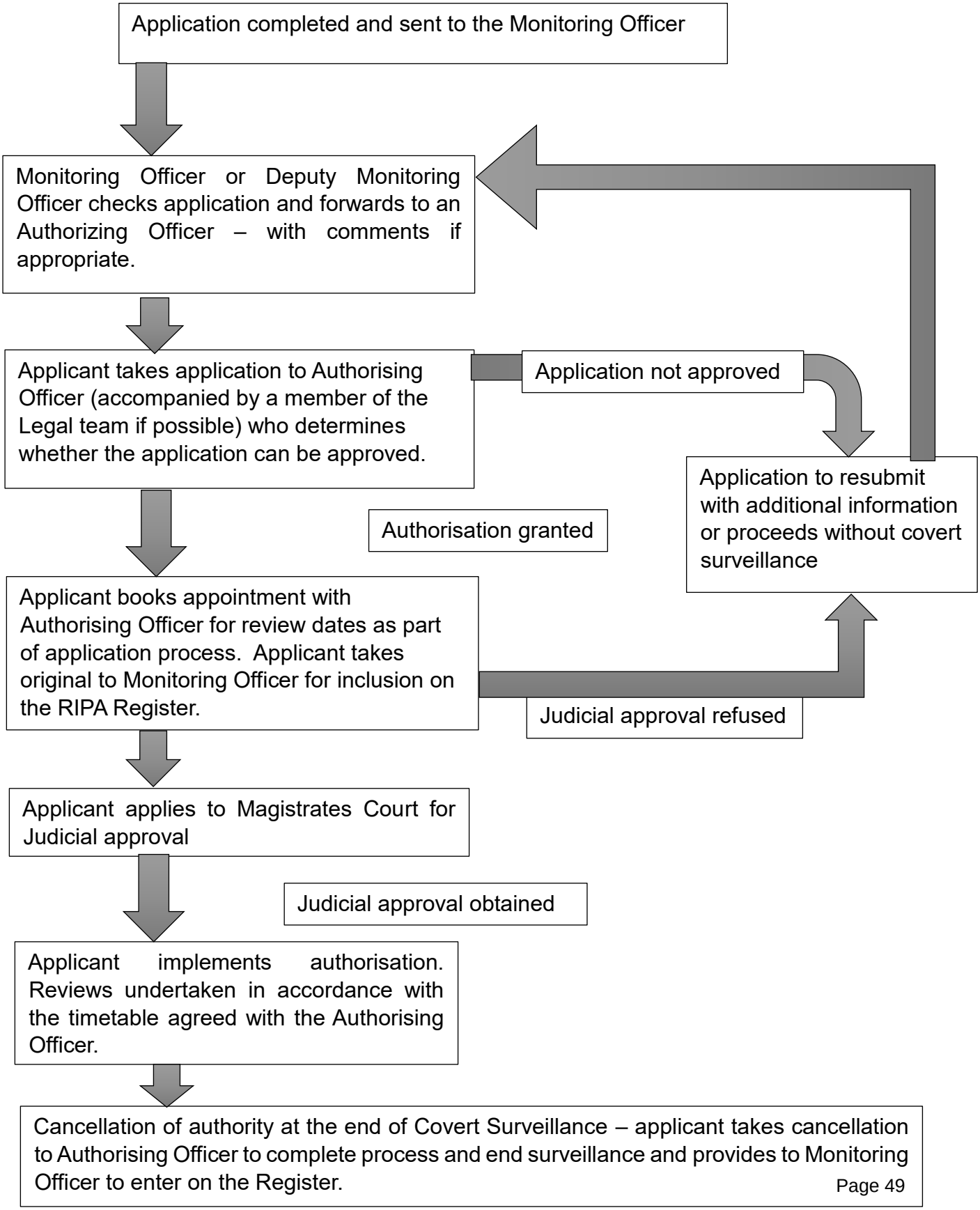
3.7.1 A joint central record of access to communications data authorisations is maintained by the Monitoring Officer at the District Council Offices, Mill Lane, Wingerworth.

3.7.2 See paragraph 2.25 for more information on the central records, which also apply in relation to covert surveillance and CHIS.

3.7.3 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.

APPENDIX A

RIPA PROCESS FLOWCHART



Appendix B

North East Derbyshire District Council

Guidance on the Use of

Social Media in Investigations

Background

The Council has an approved Corporate Policy and Procedures Document on the Regulation of Investigatory Powers Act 2000 (RIPA). For all relevant bodies, RIPA arrangements and their use fall under the oversight of the Investigatory Powers Commissioner's Office (IPCO), which assumed responsibility from the former Office of Surveillance Commissioners (OSC) in September 2017 and the Council may be subject to a periodic inspection to ensure that it complies with legislation and guidance.

In the reports for the Councils, (these were joint inspections with Bolsover District Council) both 2013-14 and 2014-15, comment was raised on the use of social networks in investigations as follows:

2013-14 report

"This is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes."

"Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remain of the view that the repeat viewing of individual 'open source' sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity."

"I strongly advise all public authorities empowered to use RIPA to have in place a corporate policy on the use of social media in investigations."

2014-15 report

"Public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices."

"I repeat my view that just because this material is out in the open, does not render it fair game. The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA and this includes repetitive viewing of what are deemed to be 'open source' sites for the purpose of intelligence gathering and data collation."

"My inspections have continued to find instances where social networking sites have been accessed, albeit with the right intentions for an investigative approach, without any corporate direction, oversight or regulation."

In August 2018, the Home Office issued its Revised Code of Practice covering Covert Surveillance and Property Interference and this now includes a section on 'online covert activity'. This guidance has been reviewed in 2024 and the guidance can be viewed at paragraph 3.10 onwards.

A copy of the full guidance can be found at: Covert surveillance and property interference code of practice (accessible) - GOV.UK

This corporate guidance document has been developed to assist officers in ensuring their investigations are carried out lawfully.

General RIPA Information

The guidance states that:-

> *"The Internet is a surveillance device as defined by RIPA section 48(1). Surveillance is covert 'if, and only if' it is conducted in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is, or may be, taking place.' Knowing that something is happening is not the same as an awareness that it is or may be taking place."*

While activity involving the use of social networks in an investigation may be deemed to be surveillance, within the meaning of RIPA (S.48(2)), not all will require a RIPA authorisation (or qualify for the protection offered through RIPA compliance – i.e. it may not reach the crime threshold).

Most cases which officers investigate will not meet the crime threshold for a RIPA authorisation. RIPA use now not only requires the internal approval of an Authorising Officer but also that of a magistrate.

This test is set out within the Council's RIPA policy.

Where a proposed investigation does not relate to an activity that meets the crime threshold, the Council expects officers to follow a similar procedure for assessment, evidencing necessity / proportionality and internal Authorising Officer review in order to provide a documented trail as a defence in the event of subsequent litigation.

Although failure to obtain appropriate authorisation or undertake a proper assessment does not render surveillance automatically unlawful, it could lead to any evidence obtained being deemed inadmissible and/or civil action taken against the Council / Officers for breach of the subject's right to privacy under Article 8 of the European Convention on Human Rights.

The Convention qualifies this right so that in certain circumstances the Council may interfere in that person's right if that interference is:- • in accordance with the law;

- necessary; **and**
- proportionate.

Depending upon the circumstances, the IPCO and the Home Office have advised that accessing or use of information found on social media, could be classed as Covert Directed Surveillance or the use of a Confidential Human Intelligence Source (CHIS) on a case by case basis:-

- Covert Directed Surveillance means surveillance which is carried out in such a way that the person(s) subject to it is unaware that it is or may be taking place.
- As a result of the Protection of Freedoms Act, from 1 November 2012 Directed Surveillance authorisations will have a crime threshold applied whereby local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.
- A person is a Covert Human Intelligence Source (CHIS) if they establish or maintain a relationship with another person in order to:-
  - covertly obtain information;
  - provide access to information to a third party; or
  - covertly disclose information obtained by the use of such a relationship and the other person is unaware that the purpose of the relationship is one of the above.

<u>Information on the Internet</u>

Online communication via the internet has, in recent years, become the preferred method of communication with other individuals, within social groups or with anyone in the world with internet access. Such communication may involve web sites, social

networks (e.g. Facebook), chat rooms, information networks (e.g. X) and/or web based electronic mail.

Just because other people may also be able to see it or access the information, does not necessarily mean that a person has no expectation of privacy in relation to that information.

Observing, monitoring and obtaining private information can amount to covert surveillance and therefore an interference with a person's right to respect for their private and family life.

Many officers and staff will have considerable experience of using the internet for their own personal online research. However managers should ensure that staff members carrying out online research and investigation for the Local Authority are both competent and appropriately trained. Any online research and investigation leaves a trace or 'footprint' and therefore safeguards need to be put in place to protect staff but also adequate procedures need to be in place to ensure such interrogation is undertaken lawfully.

Council Guidance

Open Source Research is the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within investigations.

Open Source Information is publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, journals, TV and radio broadcasts, newswires, internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports).

The Council's corporate approach is that it is acceptable for officers to undertake open source research and access open source information for the purposes of investigations / research in respect of individuals or businesses if undertaken properly, in accordance with council policy and in accordance with the law.

Investigations

If an officer during an investigation, deems it necessary and proportionate to use Open Source Research or collate Open Source Information (and such investigation does not meet the crime threshold for authorisation via RIPA), such use must be subject to adequate consideration and authorisation(s) which will depend upon the activity being undertaken.

Recording, storing and using restricted access information, in order to build up a profile of a person or a group of people must be both necessary and proportionate, and it must be retained and processed in accordance with the principles of the GDPR and DPA legislation.

Privacy Controls

The initial interaction involved in the act of bypassing privacy controls (the sending and acceptance of a friend's request) may not by itself, meet the RIPA definition of a "relationship" and will not require authorisation as a Covert Human Intelligence Source (CHIS), but such practise is discouraged. Officers are encouraged to use other means of investigating.

The creation of a false persona involving other "friends", which are also false, in order to effect the deception and secure the information effectively amounts to "legend building" in support of the CHIS and would require proper authorisations. Again this is discouraged.

Under no circumstances should an investigating officer encourage inappropriate, fraudulent or criminal behaviour in order to provoke a response as part of the use of social networking facilities in ANY of the circumstances described above.

Officers must not set up bogus accounts/identities without further discussion with the RIPA Authorising Officer and/or Legal Services and such activity will be discouraged.

Prior Notification

Unless you seek the proper authority from the Magistrates Court for permission to use covert surveillance techniques, prior notification of the use of social media in investigations should be given. Suitable wording can be provided by Legal Services

Access to Social Media Accounts

Officers should not use personal or private accounts to access social media for the purposes of investigations.

One specified Corporate Social Media Account will be used for the purposes discussed above. Such account will not use a false identity.

The communications team will monitor the sites although there will be a clear post on the site advising individuals that the site is not monitored and will redirect them to use the customer services email/telephone number.

Such site will only be used to carry out searches and not to comment, friend or "like" certain pages. Officers can screen shot information relevant to their investigation, in accordance with the table set out above and recorded in the table as set out in appendix 2.

When is Authorisation for Social Media Use Required

Research activity does not need to be authorised or recorded **except** where it relates to an investigation by any Service Area. For example, the communications team would not normally need to record their social media usage unless they are requested to access social media on behalf of another service as part of an investigation.

No social media investigations should be carried out without prior knowledge of the relevant Service Manager (where relevant) and authorisation of someone more senior than the investigating officer.

Single visit or casual research on social media does not need to be recorded, however, where there are repeated visits to a premises or visits to a specific web page or Facebook page a log should be retained and initialled by the Service Manager to confirm their authorisation for the activity.

The following should be recorded on a log with the following information:

- Officer carrying out the research
- Target of the investigation
- Date/time of viewing
- Information obtained from social platform
- Why it was considered that the viewing was necessary
- Pages saved and where saved to
- Authorisation from the Service Manager (or substitute)

The template log attached to this policy at appendix 2 should be used unless the information identified above can be recorded on a team's own "working" system (for example ECINS) so long as the information can be effectively extracted for the purposes of reporting to the IPCO or Members.

Logs will be reviewed annually by the Governance Manager on behalf of the Monitoring Officer and anonymised statistics will be reported to Members annually as part of the RIPA report.

Advice to Officers

As noted elsewhere in this guidance document, there are some grey areas over the legitimate use of social networking in investigations and the IPCO themselves have recognised that "there is a fine line between general observation, systematic observation and research."

If an Officer is considering the use of social networking for such activity, or is uncertain as to how to proceed, then further advice on the guidance and the potential RIPA requirements may be obtained from:-

- RIPA Authorising Officers
- Monitoring Officer
- Governance Manager
- Legal Services Manager

Associated Documents

This guidance is linked to a number of other Council documents which are available to staff via the Extranet:-

- RIPA Policy and Procedures Document
- Social Media Management Guidance – from Communications
- Policy on Social Networking – from Human Resources
- Links to Home Office Statutory Codes of Practice online
- 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.
- Further information on the ICO Employment Practices Code may be obtained from the Information Commissioner's Office website:- https://ico.org.uk/media/fororganisations/documents/1064/the_employment_practices_code.pdf

Appendix 1 – Extract from Home Office Code of Practice - Covert Surveillance and Property Interference
February 2024

Online covert activity

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory

purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate

messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

***Example** 1: A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

***Example** 2: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

***Example** 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or 20 operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake.

Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a
pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

***Example**: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

Extract from Home Office Code of Practice - Covert Human Intelligence Sources

December 2022

Online Covert Activity

4.29 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation. This applies whether the interaction involves publicly open websites such as an online news and social networking service, or more private exchanges such as messaging sites. Where the activity is likely to result in obtaining private information but does not amount to establishing or maintaining a CHIS relationship, consideration should be given to the need for a directed surveillance authorisation.

4.30 Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- an investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person;
- directing a member of the public to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose;
- joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.31 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required. However, consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed, and a CHIS authorisation need not be sought.

Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.32 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures

such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if there is an intention to engage in such interaction to obtain, provide access to or disclose information.

Example 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed, and no CHIS authorisation is needed.

Example 2: An officer who has maintained a false persona uses that persona to send a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be likely to be appropriate in respect of the proposed covert monitoring of the site if the activity is likely to result in obtaining private information. Once accepted into the group it becomes apparent that further interaction is necessary: this should be authorised by means of a CHIS authorisation.

4.33 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for a CHIS authorisation. Full consideration should be given to the potential risks posed by that activity.

4.34 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with paragraphs 7.15 to 7.21 of this Code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or Authorising Officer, and the extent to which this may impact on the effectiveness of oversight.

4.35 Where it is intended that more than one person will share the same online persona, each individual should be clearly identifiable within the overarching authorisation for that operation. The authorisation should provide clear information about the conduct required of – and the risk assessments in relation to – each individual involved. (See also paragraphs 3.32 to 3.36).

Appendix 2

LOG – Accessing Social Media

Officer and designation accessing social media	Date/time	Social media type	Reason/purpose/ why is it necessary?	Means of notification of access to infromation	Information retained / used	Action taken e.g. CPW, prosecution, injunction	Senior officer signature

Appendix 3

Notes (if in doubt seek advice) -

Nature of Activity	Assessment Required	Log/Records Required	Possible RIPA Authorisation
Communications Research – browsing (monitoring) 3rd party posts on social networking sites / feeds (e.g. Facebook, X/Twitter, Instagram etc.) solely for the purposes of identifying comments (positive or negative) about the Council and its activities (as is also undertaken for newspapers) is a research activity for sharing information with our residents and businesses from partner organisations such as Derbyshire Police, traffic/weather updates, community events etc.	No	No	No
Casual (one-off) examination of public posts on social networks as part of investigations undertaken	No	Yes Simple form listing sites/targets	No
Repetitive examination/monitoring of public posts as part of an investigation	Yes Authorisation from officer more senior than the investigating officer	Yes	May be classed as Directed Surveillance. Seek advice if unsure.
Examination / use of any ostensible 'private' mechanisms on social networks (e.g. as a 'friend' on Facebook, use of 'private' messaging on X (Twitter), etc.):- • within an existing relationship where the parties are known to each other, but information is freely obtained is used or	Yes Authorisation from Service Manager	Yes	Yes Directed Surveillance or the use of CHIS

passed on to an appropriate area for use in an investigation • through a new relationship set up in an open manner (i.e. in the name of the Council)			
Any Covert activity such as the following circumstances: • where a relationship is set up in a 'covert' manner specifically to obtain information • a person know to the subject becomes a 'friend', etc. specifically for the purposes of investigation • a person becomes a 'friend', etc. in a false of misleading name • where a dialogue is entered into in order to elicit information for the investigation with the subject remaining unaware (as this may be classed as entrapment).	Yes Must inform RIPA authorising officer/Monitoring Officer	Yes	Yes Directed Surveillance and/or the use of a CHIS

North East Derbyshire District Council

Standards Committee

5th March 2026

Annual Review of Whistleblowing Policy

Report of the Monitoring Officer

Classification: This report is public

Report By**:** **Andrew Smith, Deputy Monitoring Officer**

Contact Officer: **Andrew Smith, Deputy 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 5th March 2025.

A refresh and update has been undertaken and is being reported to Members.

RECOMMENDATIONS

1. Note the number of whistleblowing disclosures received in the 2025 calendar year as set out in Section 1.4.
2. Endorse the implementation actions at Section 2.6, including an annual awareness campaign and targeted training for managers, investigators and Members.
3. Approve publication of the revised policy on the Council website and intranet, and delegate authority to the Monitoring Officer to make future minor (non-material) updates to contact details and prescribed persons.
4. Approve the revised Whistleblowing Policy (Appendix 1) reflecting legal and best-practice updates set out in Section 2.

IMPLICATIONS

Finance and Risk: **Yes☐** **No ☐**

Details: Minimal direct cost; potential small costs for communications/training and graphic redraft of the flowchart can be met from existing budgets. Strengthened arrangements reduce risk of fraud, safeguarding failures and regulatory criticism.

On Behalf of the Section 151 Officer

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

Details: The updates restate statutory protections under PIDA 1998 (Public Interest Disclosure Act 1998) and the ERRA 2013 (Enterprise and Regulatory Reform Act 2013) public interest test; they also clarify safeguarding routes under the Children Act framework and Care Act 2014 statutory guidance. The Whistleblowing Register will be maintained in accordance with GDPR/Data Protection Act 2018 with defined retention, access controls and reporting. Further details as in report.

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 - £125,000 ☐ Capital - £310,000 ☐** ☒ *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
Equality Impact Assessment (EIA) details:	
Stage 1 screening undertaken • Completed EIA stage 1 to be appended if not required to do a stage 2	Not applicable
Stage 2 full assessment undertaken • Completed EIA stage 2 needs to be appended to the report	No, not applicable
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	Yes Details: Standards Committee

Links to Council Plan priorities; • **A great place that cares for the environment** • **A great place to live well** • **A great place to work** • **A great place to access good public services**
Continually improve Council Services to deliver excellence and value for money.

REPORT DETAILS

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

In accordance with the Policy, the Monitoring Officer maintains the Whistleblowing Register and reports annually to Members. For the 2025 calendar year, the number

of disclosures recorded is 0. Outcomes and learning themes (if any) will be summarised verbally at Committee and in the confidential register.

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 March 2025 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 2025 calendar year. Two disclosures were received but neither of these was a whistleblowing disclosure in relation to the actions of North East Derbyshire District Council and so they have not been recorded as whistleblowing disclosures.

2. Details of Proposal or Information

1. Summary of material changes proposed to the Policy:
    - 1.1. Add definitions section (Whistleblowing, Worker, Protected Disclosure, Public Interest test) and clarify scope for contractors, agency workers and volunteers (signposts to PIDA coverage).
    - 1.2. Strengthen reporting routes: confirm internal points of contact (Line Manager, Service Manager, Internal Audit, Monitoring Officer, Section 151 Officer, Head of Paid Service) with generic emails; allow escalation to prescribed persons and Protect (the UK whistleblowing charity).
    - 1.3. Clarify anonymous reporting: concerns will be assessed and investigated where possible, with practical guidance on evidential sufficiency.
    - 1.4. Set service standards: acknowledgment within 2 working days; decision on approach within 10 working days; proportionate updates thereafter.
    - 1.5. Explicit anti-victimisation examples and risk assessment for those raising concerns; cross-reference to Dignity at Work / Grievance policies.

1.6. Safeguarding signposts: children (Working Together to Safeguard Children 2023) and adults (Care Act 2014 statutory guidance) – such concerns may need immediate referral via statutory pathways.

1.7. Data protection and records: describe Whistleblowing Register governance, access, retention and GDPR basis; annual reporting to Standards/Audit Committee.

1.8. Remove legacy references (e.g., Audit Commission) and update external contacts (External Auditor, Police) using role-based rather than named contacts.

1.9. Redraw and replace the flowchart for clarity and accessibility (high-resolution version).

2. Implementation actions and timeline:
   2.1. Publish updated policy and quick- read one- page guide on intranet/website within 10 working days of approval.
   2.2. Briefing note to all staff and Members; targeted sessions for managers and investigators within 8 weeks.
   2.3. Update contact points (generic emails) and set up shared mailbox for whistleblowing disclosures.
   2.4. Replace flowchart on website and in staff handbook; ensure accessibility compliance (WCAG 2.2 AA).
   2.5. Schedule annual metrics report to Standards Committee (number and themes; no identifying information).

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

4. The policy, once approved by Standards Committee, will be on the Council's website.

3 Reasons for Recommendation

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

3.2 There are no instances of Whistleblowing to report to 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	Whistleblowing Policy April 2026

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

APPENDIX A – Summary of policy changes for 2026 review

Definitions and scope clarified; expanded coverage signposted for workers under PIDA.

Updated reporting routes and contact points; inclusion of Protect as an external advice route.

Anonymous reporting handling clarified.

Service standards for handling concerns introduced.

Anti- victimisation safeguards expanded with examples.

Safeguarding signposts (children and adults) strengthened.

Register and data governance set out; annual reporting to Committee.

Obsolete references (Audit Commission) removed; external contacts modernised.

Flowchart replaced with accessible, high- resolution version.

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 –	Approved
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
Final Policy approval route (i.e. Executive/Council Committee)	Standards Committee
Date Policy approved	Last approved 5 March 2025

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

WHISTLEBLOWING POLICY

1. Introduction

1.1 Employees, Members, contractors and others engaged in Council business 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. Definitions

2.1 Whistleblowing

Reporting a concern that the whistleblower reasonably believes is made in the public interest and tends to show one or more of the following:

- A criminal offence
- A breach of legal obligation

- A miscarriage of justice
- A danger to health and safety
- Damage to the environment
- Deliberate concealment of wrongdoing

2.2 Worker

For the purposes of whistleblowing law (Public Interest Disclosure Act 1998), this includes employees, agency workers, contractors, trainees, and other individuals working under the Council's direction.

2.3 Protected Disclosure

A disclosure that meets the public interest test, relates to qualifying wrongdoing, and is made through an appropriate channel

2.4 Public Interest Test

A disclosure must be made in the reasonable belief of the individual that it serves the public interest

3. Aims and Purpose of this Policy

3.1 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.

4. Scope of the Policy

4.1 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

4.2 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.

5. When this Policy may not be appropriate

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

6. Safeguards against Harassment or Victimisation

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.

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

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

6.2 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.

7. Confidentiality

7.1 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.

8. Anonymous Allegations

8.1 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.

8.2 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.

9. Untrue Allegations & Legal Protection

9.1 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.

9.2 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.

9.3 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.

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

10. How to raise a Concern under this Policy

10.1 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 and why the matter is of public interest.
- Submit any relevant evidence or documentation.

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

10.3 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.

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

Employees

10.5 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

10.6 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)

10.7 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

10.8 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.

10.9 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 Safeguarding Concerns

10.1 If the concern involves:

- Children follow Working Together to Safeguard Children (2023) processes
- Adults at risk: follow Care Act 2014 safeguarding duties

10.2 Such matters bypass whistleblowing and be referred immediately to statutory authorities.

11 The Responsible Officer

11.1 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.

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

11.3 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.

13. Appendix- Quick Reference Summary

13.1 What to report

- Serious wrongdoing, risk or malpractice affecting others.

13.2 How to report

- Manager, Service manager, internal Audit, Monitoring Officer, Section 151 Officer, Head of Paid Service.
- Or external bodies (Prescribed Persons, Police, External Auditor, Protect)

13.3 Protections

- Protection from detriment
- Confidentiality where possible
- Anoymous reports considered

13.4 Timesclaes

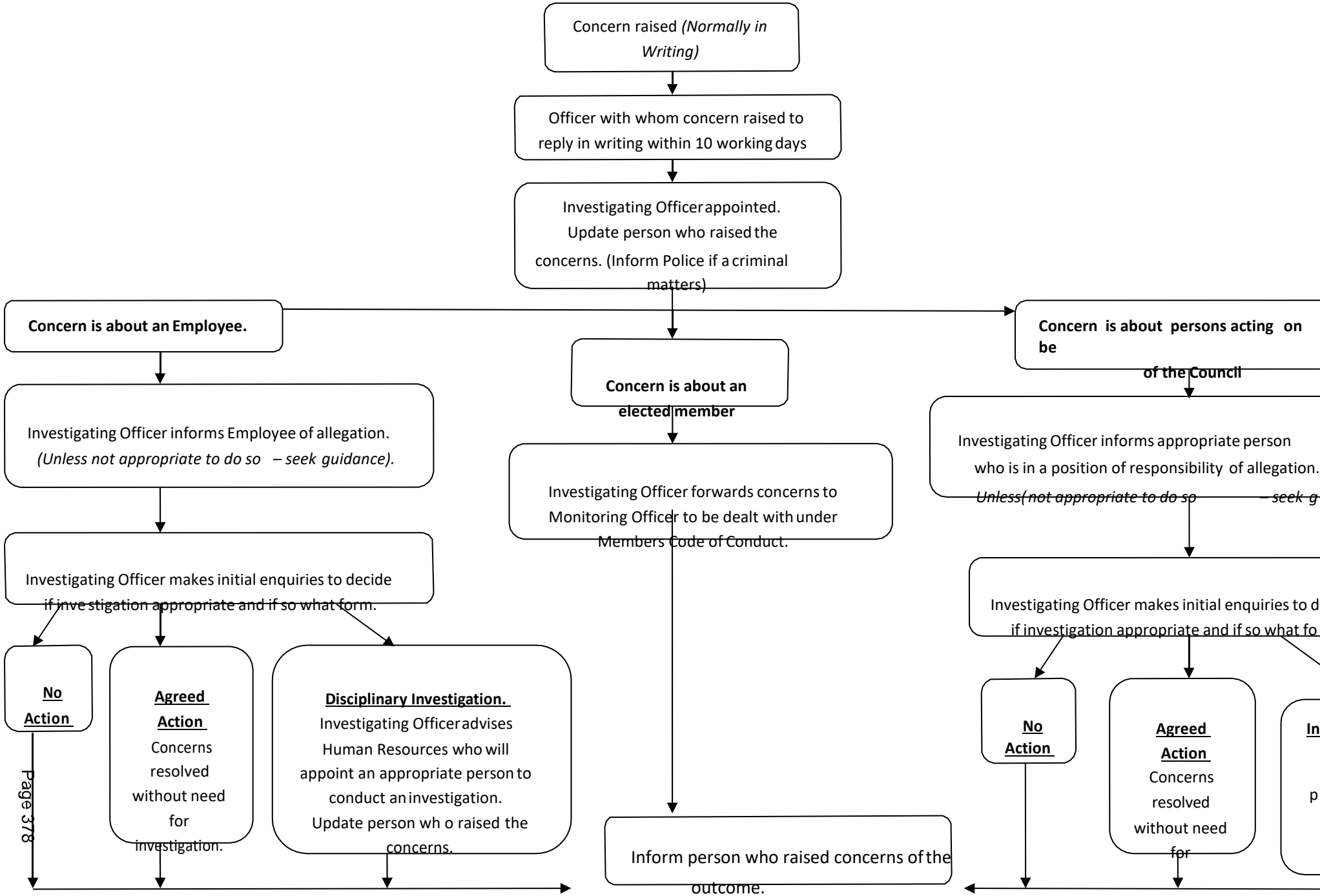
- Initial decision: 10 working days

13.5 Annual Reporting

- Monitoring Officer maintains the Register and reports anonymized data to Standards/Audit Committee

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 responsibility 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 fo
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.
No Action
Agreed Action Concerns resolved without need for
In
p
Inform person who raised concerns of the outcome.

North East Derbyshire District Council

Standards Committee

29th April 2026

Social Media Guidance for Councillors – Appendix 5 of the Constitution

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

To seek Members comments on the revised version of the Social Media Guidance for Members and to seek approval for referral to Council for approval.

RECOMMENDATIONS

1. That Members comment on the draft and recommend it to Council for inclusion in the 2026 Constitution.
2. That once approved by Council, the Chair of Standards Committee and the Monitoring Officer email all Members with the new version and clarify the requirement for Members to follow the guidance as part of the ethical framework.
3. Training is made available to all Members.

IMPLICATIONS

Finance and Risk: **Yes☐** **No ☒**

Details: This is guidance for Members and has no financial consequences in itself.

On Behalf of the Section 151 Officer

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

Details: As in the report.

On Behalf of the Solicitor to the Council

Staffing: **Yes☐** **No ☒**

Details: There is no direct impact on staff. However bullying and harassment of staff or anyone else, is covered within the guidance**.**

On behalf of the Head of Paid Service

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 - £125,000 ☐ Capital - £310,000 ☐** ☒ *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
Equality Impact Assessment (EIA) details:	
Stage 1 screening undertaken • Completed EIA stage 1 to be appended if not required to do a stage 2	Yes, appended.
Stage 2 full assessment undertaken • Completed EIA stage 2 needs to be appended to the report	No, not applicable
Consultation: **Leader / Deputy Leader ☐ Cabinet ☐** **SMT ☐ Relevant Service Manager ☐** **Members ☐ Public ☐ Other ☐**	Yes Details: The Statutory Officers and Directors (SOD) and the Standards Committee have been consulted.

Links to Council Plan priorities; • **A great place that cares for the environment** • **A great place to live well** • **A great place to work** • **A great place to access good public services**
All indirectly

REPORT DETAILS

1 Background *(reasons for bringing the report)*

1.1 As Members are aware, each year the Council's Constitution is reviewed by the Standards Committee. However the Social Media Guidance for Councillors needs a more thorough review in the light of current knowledge of the usage of social media and the risks and advantages of its use and in the light of new LGA guidance.

1.2 This year the guidance has been reviewed by the Communications and Marketing Manager from a communications point of view, as well as by myself. This means that the Communications Team's own practical experience of using social media can be fed into the revised guidance.

1.3 This includes definitions of and explanations of misinformation, disinformation, and malinformation as well as what is expected from Councillors using social media.

1.4 The LGA has produced a lot of guidance for Members on the use of and dangers of social media. The link to this is included at the end of the guidance for easy access for Members.

1.5 Part of this is the Digital citizenship 'rules of engagement' with infographics and text which can be added to any Social Media pages. These set out the expectations of users of the Social Media website in terms of behaviour and debate. The Link is: Digital citizenship: support and resources for councillors | Local Government Association

2. Details of Proposal or Information

2.1 The draft Guidance is attached for Members to consider.

2.2 In terms of promoting this guidance, following the Annual Meeting's approval of the revised draft Guidance, it is suggested that the Chair of Standards Committee and the Monitoring Officer jointly email all Members with the new version and outline the requirement for Members to follow the guidance.

2.3 In addition, following approval at the Annual Meeting, there is a need to carry out some social media training of Members. Members views on how best this can be done are welcome.

3 Reasons for Recommendation

3.1 To ensure Members have the latest guidance and are able to attend suitable training.

4 Alternative Options and Reasons for Rejection

4.1 It is not an option to decide not to review a part of the Constitution.

DOCUMENT INFORMATION

Appendix No	Title
1	Draft Social Media Guidance for Councillors
2	Equality Impact Assessment

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

D

North East Derbyshire District Council

Stage 1 – Equality Impact Assessment Screening

Any new policy, strategy, function, service, practice, or proposal will need to be screened to decide whether it's relevant to equality and if this is the case, it is necessary to build an assessment (Stage 2) into the **initial drafting** or **development** of the piece of work.

The relevant strands of equality are:

Age, Disability, Gender identity/Gender reassignment, Race, Religion or belief, Sex, Sexual orientation, Women who are pregnant or have recently had a baby.

Also, for issues affecting staff, consider employees who are married or in a civil partnership.

The next section sets out the points you may need to consider in determining whether to carry out an EIA (stage 2). For advice/support in making this determination, please contact the Information & Improvement Team (Equality lead).

For more information how to complete this form please refer to the Guidance which can be found at HERE

Title of policy or proposal	Social Media Guidance for Councillors which is part of the Constitution.
Name of EIA lead	Sarah Sternberg
Briefly describe the aims of the policy, strategy, service, decision or proposal, its aims, the likely outcomes, and the rationale for it	This provides social media guidance for Councillors explaining the risks and benefits of using social media. It makes clear how to use them safely (for themselves and for the Council), what not to do when using them, being respectful and how to manage content.

	Initial Assessment Considerations	Yes	No	Comments
1.	Does this policy/proposal affect people: • Customers • Residents • Staff	**Yes**		**These groups are affected as potential recipients of the Councillors' social media posts. This guidance aims to give Councillors the tools to ensure that the social media posts they make do**

	Initial Assessment Considerations	Yes	No	Comments
				not affect these groups.
2.	Does it have the potential to adversely impact on any of the protected characteristics?		**No**	**The guidance doesn't. However the social media posts could so affect protected characteristics.**
3.	Can the council influence the impact? E.g., is it a statutory requirement, national guidance etc.		**No**	**By producing this guidance the Council is giving the Members the tools to ensure that there is no impact.**
4.	Are existing equality monitoring processes already in place? If so, please note under comments		**No**	**This isn't applicable. Members social media posts aren't monitored.**

If the answer to questions 1 to 3 above is 'yes', then an **Equality Impact Assessment** (Stage 2) may be necessary.

A copy of the form should be sent via email to the Information and Improvement (Equality Lead) amar.bashir@ne-derbyshire.gov.uk and a copy should be retained with your policy/proposal documentation.

Equality Officer Recommendation	Tick as appropriate	Date
EIA Stage 2 required		
EIA Stage 2 NOT required	No	13.4.2026

Copy to be returned to the EIA lead with Equality Officer recommendation.

Information and Improvement Team to keep a central electronic record of all decisions made under Stage 1.

Appendix 5
Social Media Guidance for Councillors

1. Introduction

1.1 Social media enables councillors to communicate directly with residents, businesses and stakeholders, increasing engagement and transparency in local democracy.

1.2 It increases our access to audiences and improves the accessibility of our communication. It enables us to be more active in our relationships with citizens, partners and stakeholders and encourages people to be involved in local decision making, enabling better engagement and feedback, ultimately helping to improve the services we provide.

1.3 At the same time, social media presents specific risks to public trust, individual safety, exposure of the Council to security risks and risks to the Council's reputation due to the speed, scale and permanence of online communication.

1.4 This guidance supports Councillors to use social media confidently and responsibly, while meeting the standards set out in the Members' Code of Conduct and complying with Data Protection and other legislation. It provides practical clarity on expectations in modern online environments.

2. Policy Statement

2.1 This guidance provides a structured approach to using social media and will ensure that the use of social media is effective, lawful and does not compromise Council information or computer systems/networks.

2.2 Users must ensure that they use social media sensibly and responsibly, in line with corporate policy. They must ensure that their use will not adversely affect the Council or its business, nor be damaging to the Council's reputation and credibility or otherwise violate any Council policies.

3. Status of this guidance

3.1 This document is supplementary guidance and must be read alongside the Members' Code of Conduct.

3.2 Breaches of this guidance may amount to a breach of the Code of conduct, depending on the circumstances.

3.3 The guidance is intended to:

- support good judgement,
- prevent harm and escalation,
- and enable early, informal resolution where possible.

4 Risks

4.1 The following risks have been identified with social media use (this is not an exhaustive list):

- Virus or other malware (malicious software) infection from infected sites.
- Disclosure of confidential information.
- Damage to the Council's reputation.
- Social engineering attacks (also known as 'phishing').
- Bullying or "trolling". An internet "troll" is a person who starts arguments or upsets people, by posting inflammatory or off-topic messages online with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal discussion, often for their own amusement.
- Civil or criminal action relating to breaches of legislation.
- Breach of safeguarding through the use of images or personal details leading to the exploitation of vulnerable individuals.
- Breach of the Code of Conduct for Members through inappropriate use.

4.2 In light of these risks, the use of social media sites should be regulated to ensure that such use does not damage the Council, its employees, councillors, partners and the people it serves. As such this guidance aims to ensure:

- A consistent and corporate approach is adopted and maintained in the use of social media.
- Council information remains secure and is not compromised through the use of social media.
- Users operate within existing policies, guidelines and relevant legislation.
- The Council's reputation is not damaged or adversely affected.

5 Scope

5.1 This guidance applies to all forms of online communication, including (but not limited to):

- Facebook pages and profiles
- X (Twitter), Instagram, LinkedIn
- blogs, forums and comment threads
- video and livestream platforms

5.2 The guidance applies whether a Councillor is using:

- an account created specifically for their councillor role, or
- a personal account where council business is discussed.

Residents will generally assume Councillors are acting in their official capacity when commenting on Council matters online.

6 Core responsibilities of Councillors online

6.1 When using social media in connection with Council business, Councillors are expected to:

- act with integrity, honesty and reasonable care
- treat others with respect and dignity
- avoid conduct that could reasonably bring the Council into disrepute
- uphold public confidence in lawful decision-making and governance
- abide by the Nolan Principles and the Code of Conduct

These principles apply equally online as they do in meetings or written correspondence.

6.2 Councillors are personally responsible for the content they publish on any form of social media. Publishing or allowing to be published (in the form of a comment) an untrue statement about a person which is damaging to their reputation may incur a libel action for which the individual Councillor will be personally liable.

6.3 Social media sites are in the public domain and it is important to ensure you are confident of the nature of the information you publish. Once published, content is almost impossible to control and may be manipulated without your consent, used in different contexts, or further distributed.

7. Information integrity: misinformation, disinformation and malinformation

7.1 Definitions

- Misinformation: inaccurate or incorrect information shared without intent to mislead.
- Disinformation: inaccurate information shared deliberately to mislead or inflame.
- Malinformation: information that may be true or partly true, but is shared selectively, without material context, or in a way that misleads or causes harm.

7.2 Why malinformation matters most

Malinformation presents a particular risk because:

- it can appear credible and authoritative,
- it is harder to correct than outright falsehoods,
- and it can significantly damage trust while remaining technically “true”.

Councillors should therefore take particular care with framing, tone, timing and context, not just factual accuracy.

7.3 The following are illustrative examples of what is likely to constitute malinformation:

- selectively listing negative facts to imply systemic failure while omitting relevant context or constraints
- reframing a lawful or factual Council clarification as evidence of coercion, bad faith or wrongdoing
- presenting speculation about motives or intent as established fact
- quoting partial extracts from reports, emails or statements in a way that changes their meaning

7.4 Examples that are not malinformation

- clearly labelled opinion or political disagreement
- robust criticism of decisions or processes that fairly reflects the known facts
- calling for transparency or scrutiny without emotive or misleading framing

8. Tone, respect and dignity of office

8.1 Councillors are entitled to challenge decisions and policies robustly. Healthy debate is a core part of democracy.

8.2 However, councillors should avoid language that:

- ridicules or mocks individuals
- undermines credibility or agency through insinuation
- frames lawful governance actions as inherently untrustworthy
- encourages contempt rather than scrutiny

8.3 This applies even where language falls short of explicit bullying or harassment. The test is whether a reasonable member of the public would see the behaviour as undermining dignity, respect or trust.

9. Scale, reach and amplification

9.1 Councillors should be mindful that:

- individual social media accounts may reach audiences larger than official Council channels
- repeated posting can dominate narratives and shape public perception
- impact is driven by amplification as well as content

9.2 Greater reach carries greater responsibility. Councillors should therefore exercise increased care when posting about live, sensitive or complex issues.

10. Managing comments and duty of care

10.1 Why comment management matters

Where a councillor publishes a post relating to Council business, they are responsible for the space they control.

Leaving abusive or threatening comments visible can:

- normalise harassment
- encourage escalation and pile-on behaviour
- be reasonably interpreted as tolerating such conduct

This engages the standards of respect, integrity and public confidence set out in the Code of Conduct.

10.2 Reasonable steps expectation

Councillors are not expected to police disagreement or remove criticism.

However, where comments under a post include abuse, harassment or threats, Councillors are expected to take reasonable and proportionate steps, such as:

- removing or hiding comments that are abusive, threatening or hateful
- posting a clear boundary-setting message (e.g. “Debate is welcome; abuse or threats are not”)
- reporting comments that breach platform rules
- escalating credible threats through appropriate channels (Monitoring Officer / Police)

10.3 What may constitute a failure to moderate

Examples include:

- leaving visible personal insults or harassment while actively engaging in the thread
- allowing repeated abusive comments to remain unchallenged
- permitting language that encourages intimidation or hostility to escalate

Each case will depend on context, but inaction in the face of foreseeable harm may amount to a breach of the Code of Conduct.

11. Confidentiality, data protection and safeguarding

11.1 Councillors must not disclose confidential or exempt information online.

11.2 Personal data must be handled in line with data protection legislation.

11.3 Safeguarding responsibilities apply online. Concerns about exploitation, threats or vulnerable individuals should be reported promptly.

12. Personal safety and separation of roles

12.1 Councillors are strongly encouraged to maintain separate accounts for:

- councillor duties, and
- personal or family life.

12.2 Privacy settings should be used appropriately, but Councillors should assume that anything posted may become public.

12.3 Don't share personal information such as your personal phone number, date of birth, home address – or photos that make any of these obvious

13. If in doubt: pause and seek advice

13.1 If you are unsure whether a post:

- could mislead through framing or omission,
- relates to a live or sensitive issue,
- risks escalation or abuse in comments,

pause and seek advice from the Monitoring Officer before posting.

Early advice is always preferable to formal investigation.

14. Breaches and consequences

14.1 Serious or repeated breaches of this guidance may amount to a breach of the Members' Code of Conduct.

14.2 Some breaches (e.g. defamation, discriminatory language, data protection, electoral law) may also result in personal civil or criminal liability.

15 Key takeaway (the golden rule)

If you wouldn't say it in a public meeting, or allow it to be said unchecked in a room you were chairing, don't publish it — or leave it standing — online.

16. Guidance on Capturing Social Media Posts

16.1 Posts made using third party sites such as Facebook or X are not held by and are not within the control of the Council - posts can be deleted by site administrators without the knowledge or consent of the Council. In exceptional circumstances, copies of posts may be made and retained by the Council, in line with relevant Council procedures. These copies will be held for a period dependent on the type of investigation they are subject to.

16.2 Where inappropriate use is suspected, it is suggested that you should pro-actively attempt to capture any inappropriate posts before they might be deleted. Copies should be made and reported to the Monitoring Officer within the Council, as well as following the social media sites own reporting procedures where appropriate.

Dos and Don'ts

- Do make use of stringent privacy settings if you don't want your social media to be accessed by the press or public. Read the terms of service of any social media site accessed and make sure you understand their confidentiality/privacy settings.

- Do not disclose personal details such as home addresses and telephone numbers. Ensure that you handle any personal or sensitive information in line with the Council's Data Protection Policy.

- Safeguarding issues are paramount because social media sites are often misused by offenders. Safeguarding is everyone's business – if you have any concerns about other site users, you have a responsibility to report these.

- Do not publish or report on meetings which are private or internal (where no members of the public are present or it is of a confidential nature) or exempt reports (which contain confidential information or matters which are exempt under the provision of the Local Government (Access to Information) Act 1985).

- Copyright laws still apply online. Placing images or text from a copyrighted source (e.g. extracts from publications or photos) without permission is likely to breach copyright. Avoid publishing anything you are unsure about or seek permission from the copyright holder in advance.

- Don't send or post inappropriate, abusive, bullying, hateful or defamatory messages to members of the public, other Councillors or Officers either in or outside the work environment. This includes content relating to protected characteristics, including but not limited to race, religion or belief, disability, sexual orientation, gender reassignment, sex or age.

- The account should state that the views are those of the Councillor and that these may not represent the views of the Council.

- Do not use the Council's logo, or any other Council related material on a personal account or website.

- Social media must not be used for actions that would put Councillors in breach of the Council's Code of Conduct for Members. For example, don't publish on social media something you wouldn't say face to face, or at a public meeting.

- Be aware of your own safety when placing information on the internet and do not publish information which could leave you vulnerable.

- Anyone receiving threats, abuse or harassment via their use of social media should report it to their political group leader, the Monitoring Officer and the Police.

- Where someone has posted a hateful or discriminatory comment on your personal blog or social media account, do inform the site administrator as soon

as you become aware of the comment and consider reporting the matter to the Police.

- Do abide by the special rules that apply to social media posts and blogs during a local election period.

Further guidance is available for Councillors from the LGA. There is extensive guidance on their website on this link google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjggMzvgOuTAxXLUUEAHXWSG_UQFnoECA4QAQ&url=https%3A%2F%2Fwww.local.gov.uk%2Four-support%2Fcommunications-and-community-engagement%2Fsocial-media-guidance-councillors&usg=AOvVaw1G1pXhdtAld2ZSSJMKliT4&opi=89978449

And in particular, there is guidance on infographics and rules of use of the Social Media website at Digital citizenship: support and resources for councillors | Local Government Association These can be added to the front page of Councillors' Social Media to make other users clear what acceptable behaviour is expected.

North East Derbyshire District Council

Standards Committee

29 April 2026

DISCIPLINARY PROCEDURE FOR STATUTORY OFFICERS

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: Amy Bryan – Governance Manager

PURPOSE / SUMMARY

This report sets out a revised procedure to be followed in relation to the disciplinary procedure for the Council's Statutory Officers, including revisions to the Employment and Appeals Committee structure.

RECOMMENDATIONS

1. That the revised disciplinary procedure for Statutory Officers be approved.

2. That the revised Terms of Reference for the Employment and Appeals Committee, including the establishment of an Investigation and Disciplinary Committee, be approved.

3. That the Chief Executive Officer be granted delegated authority to make minor non-material changes to the procedure as required.

IMPLICATIONS

Finance and Risk: **Yes**☐ **No** ☒

Details: There are no financial or risk implications arising from this report.

On Behalf of the Section 151 Officer

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

Details: The disciplinary procedure for statutory officers must comply with the requirements of the Local Authorities (Standing Orders) (England) Regulations 2001, as amended by the Local Authorities (Standing Orders) (England) (Amendment) Regulations 2015. These regulations prescribe mandatory protections for statutory officers, including the requirement that any proposal to dismiss the Head of Paid Service, Monitoring Officer or Chief Finance Officer must be considered by an Independent Panel prior to a final decision by Full Council.

The procedure must also reflect the authority's obligations as an employer. Failure to follow a procedurally fair process could expose the authority to claims for unfair dismissal on the grounds of procedural irregularity.

On Behalf of the Solicitor to the Council

Staffing: **Yes☐** **No ☒**
Details: None arising from this report.

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 - £125,000 ☐ Capital - £310,000 ☐** ☒ *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

Equality Impact Assessment (EIA) details:	
Stage 1 screening undertaken • Completed EIA stage 1 to be appended if not required to do a stage 2	Yes, appended
Stage 2 full assessment undertaken • Completed EIA stage 2 needs to be appended to the report	No, not applicable
Consultation: **Leader / Deputy Leader ☒ Cabinet ☐** **SMT ☐ Relevant Service Manager ☒** **Members ☐ Public ☐ Other ☐**	Yes Details:

Links to Council Plan priorities; • **A great place that cares for the environment** • **A great place to live well** • **A great place to work** • **A great place to access good public services**

REPORT DETAILS

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

1.1 It is best practice to have the appropriate structures and standing committees in place in order that potential disciplinary issues can be quickly addressed.

1.2 The Local Authorities (Standing Orders) (England) Regulations 2001 (as amended by the Local Authorities (Standing Orders) (England) (Amendment) Regulations 2015 made changes to the matters relating to the dismissal of the three Statutory Officers, the Head of Paid Service, Monitoring Officer and Section 151 Officer (the Relevant Officers).

2. <u>Details of Proposal or Information</u>

2.1 The proposed process for dealing with allegations against Statutory Officers is set out in Appendix 1.

2.2 The disciplinary procedure for statutory officers must be implemented in line with the Council's responsibilities as an employer and with established principles of fair and reasonable treatment. This includes ensuring that Statutory Officers who are subject to the procedure are treated fairly, kept

informed at each stage of the process, and provided with reasonable opportunities to respond to concerns raised.

2.2 The proposed changes to the Terms of Reference of the Employment and Appeals Committee (EAC) are set out in Appendix 2. This includes the creation of a second Committee – the Investigation and Disciplinary Committee (IDC).

2.3 The IDC will have a different membership to the EAC, to enable it to consider preliminary investigation reports, determine whether further action is required (including formal investigation and appointment of external investigator), make recommendations to full Council and to deal with the final stages of the grievance procedures for all Statutory Officers.

2.4 The Employment and Appeals Committee will deal with hearing appeals against the decision of the IDC in respect of action short of dismissal (written warning or final written warning).

3 Reasons for Recommendation

3.1 To ensure the Council has a robust process in place.

4 Alternative Options and Reasons for Rejection

4.1 To do nothing. This has been rejected as the Council's needs a robust procedure for any allegations against Statutory Officers.

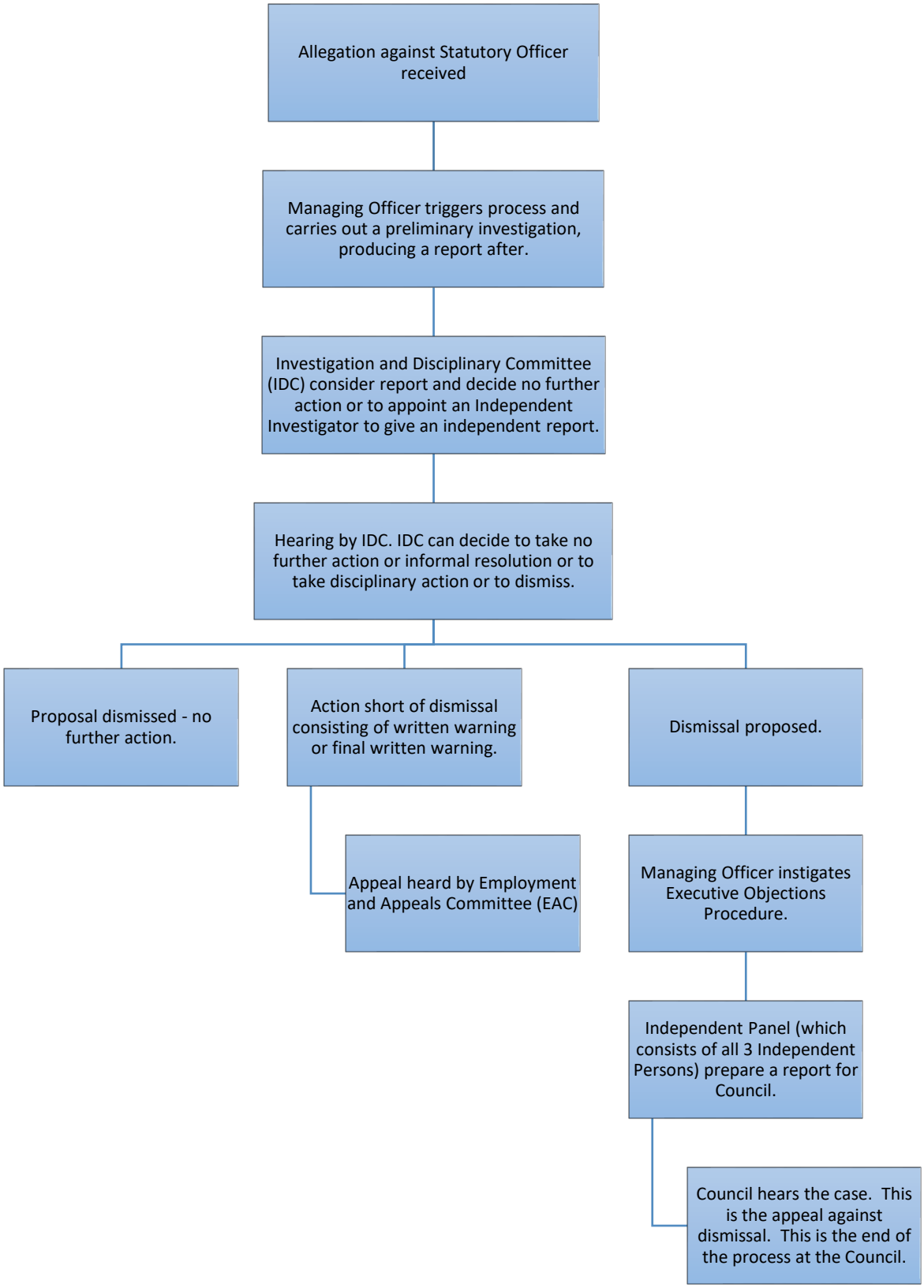
DOCUMENT INFORMATION

Appendix No	Title
1	Statutory Officer Allegations Process
2	Proposed Terms of Reference
3	EIA Stage 1

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)

Model Disciplinary Procedure for Chief Executives agreed by the JNC for Chief Executives of Local Authorities as updated in September 2022.

Statutory Officer Allegations Process



Proposed Updated Terms of Reference for Employment and Appeals Committee

Employment and Appeals Committee and Investigation and Disciplinary Committee

There will be an Employee and Appeals Committee of four Councillors.

The membership shall comprise the Leader of the Council, the Deputy Leader, a Cabinet Member and the Leader of the Largest Minority Group or their appointed substitute.

There will be an Investigation and Disciplinary Committee of four Councillors.

The membership shall comprise of three Cabinet members and the Deputy Leader of the Largest Minority Group or their appointed substitute.

Substitutes if called upon will replace an existing member for the duration of an employment procedure in its entirety. At its conclusion, appointment reverts to the Member originally appointed.

The Members shall be appointed at the Annual Meeting. The rules of proportionality shall apply to this Committee.

The two Committees will have the roles and functions as set out below:

EMPLOYMENT AND APPEALS COMMITTEE
To interview candidates for posts within the Senior Management Team. To appoint candidates to posts within the Senior Management Team, with the exception of the Head of Paid Service, Chief Finance Officer and Monitoring Officer. To recommend to Council the appointment of the Head of Paid Service, Chief Finance Officer and Monitoring Officer. To deal with appeals from the Chief Officers/Deputy Chief Officers, including Statutory Officers, against action taken against them.

INVESTIGATION AND DISCIPLINARY COMMITTEE
To deal with the final stages of the grievance and harassment procedures for all Statutory Officers and other Chief Officers/Deputy Chief Officers. To determine whether to appoint an Independent Investigator to give an independent report regarding a complaint against a Statutory Officer. In respect of the dismissal of any of the Statutory Officers, namely the Head of Paid Service, the Monitoring Officer and the Section 151 Officer, the Investigation and Disciplinary Committee shall make a recommendation to Council which will be supported via a report from two of the Council's Standards Committee Independent Persons.

D

North East Derbyshire District Council

Stage 1 – Equality Impact Assessment Screening

Please download this form and save as

Any new policy, strategy, function, service, practice, or proposal will need to be screened to decide whether it's relevant to equality and if this is the case, it is necessary to build an assessment (Stage 2) into the **initial drafting** or **development** of the piece of work.

The relevant strands of equality are:

Age, Disability, Gender identity/Gender reassignment, Race, Religion or belief, Sex, Sexual orientation, Women who are pregnant or have recently had a baby.

Also, for issues affecting staff, consider employees who are married or in a civil partnership.

The next section sets out the points you may need to consider in determining whether to carry out an EIA (stage 2). For advice/support in making this determination, please contact the Information & Improvement Team (Equality lead).

For more information how to complete this form please refer to the Guidance which can be found at HERE

Title of policy or proposal	Disciplinary Procedure for Statutory Officers
Name of EIA lead	Amy Bryan – Governance Manager
Briefly describe the aims of the policy, strategy, service, decision or proposal, its aims, the likely outcomes, and the rationale for it	A revised procedure in relation to the disciplinary procedure for the Council's Statutory Officers, including revisions to the Employment and Appeals Committee structure. The disciplinary procedure for statutory officers must be implemented in line with the Council's responsibilities as an employer and with established principles of fair and reasonable treatment. This includes ensuring that Statutory Officers who are subject to the procedure are treated fairly, kept informed at each stage of the process, and provided with reasonable opportunities to respond to concerns raised.

	Initial Assessment Considerations	Yes	No	Comments
1.	Does this policy/proposal affect people: • Customers • Residents • Staff	✓		Affects a very small number of staff

	Initial Assessment Considerations	Yes	No	Comments
2.	Does it have the potential to adversely impact on any of the protected characteristics?		✓	
3.	Can the council influence the impact? E.g., is it a statutory requirement, national guidance etc.	✓		The Council sets the procedure, but it might comply with legislation, and the proposal follows the Model Procedure.
4.	Are existing equality monitoring processes already in place? If so, please note under comments	✓		The procedure must reflect the authority's obligations as an employer and existing monitoring for staff procedures remain the same.

If the answer to questions 1 to 3 above is 'yes', then an **Equality Impact Assessment** (Stage 2) may be necessary.

A copy of the form should be sent via email to the Information and Improvement (Equality Lead) amar.bashir@ne-derbyshire.gov.uk and a copy should be retained with your policy/proposal documentation.

Equality Officer Recommendation	Tick as appropriate	Date
EIA Stage 2 required	✓	20/04/2026
EIA Stage 2 NOT required		

Copy to be returned to the EIA lead with Equality Officer recommendation.

Information and Improvement Team to keep a central electronic record of all decisions made under Stage 1.

STANDARDS COMMITTEE 2025/26 – WORK PROGRAMME

Date	Agenda items
10 December 2025	• Annual Complaint Performance and Service Improvement Report for Housing • Government response to consultation on strengthening the standards and conduct framework for local authorities in England • Request for Dispensation • Review of the Constitution
25 February 2026	• Gifts and Hospitality Annual Report • Review of the Constitution • Code of Conduct - update on recent cases • Standards Sub-Committee Hearing Procedure • Member Officer Protocol • Complaints Update
29 April 2026	• Review of the Constitution • Review of Members' Attendance at Training Events • RIPA Policy Annual Report • Whistleblowing Policy Annual Report • Planning Site Visit Protocol • Social Media Guidance • Disciplinary Procedure for Statutory Officers • Meeting Times