STANDARDS COMMITTEE

AGENDA

Tuesday 5th September 2017 at 1400 hours in the Council Chamber, The Arc, Clowne

Item No.		Page No.(s)
	PART 1 – OPEN ITEMS.	
1.	**Apologies for absence**	
2.	**Urgent Items of Business** To note any urgent items of business which the Chairman has consented to being considered under the provisions of Section 100(B) 4 (b) of the Local Government Act 1972.	
3.	**Declarations of Interest** Members should declare the existence and nature of any Disclosable Pecuniary Interest and Non Statutory Interest as defined by the Members' Code of Conduct in respect of: a) any business on the agenda b) any urgent additional items to be considered c) any matters arising out of those items and if appropriate, withdraw from the meeting at the relevant time.	
4.	To approve the minutes of a meeting held on 13th April 2017.	3 to 5
5.	Review of Protocol on Member/Officer Relations.	6 to 14
6.	Review of Joint Regulation of Investigatory Powers Act (RIPA) Policy.	15 to 44
7.	Update on Independent Person Recruitment.	Verbal Update
8.	Complaints of Breach of the Code of Conduct – 2017.	Verbal Update
9.	Work Plan 2017/18.	45 to 48

STANDARDS COMMITTEE

Minutes of a meeting of the Standards Committee of the Bolsover District Council held in the Council Chamber, The Arc, Clowne, on Thursday, 13 April 2017 at 1000 hours.

PRESENT:-

Members:- Councillors G Buxton, H J Gilmour, C R Moesby and B Watson.

Mrs R Jaffray in the Chair

Officers:- S E A Sternberg (Monitoring Officer), A Wylie (Deputy Monitoring Officer) and N Calver (Governance Manager).

0905. APOLOGIES FOR ABSENCE

Apologies for absence were submitted on behalf of Mr Stephen Wainwright, Independent Person.

0906. URGENT ITEMS OF BUSINESS

There were no urgent items of business to consider.

0907. DECLARATIONS OF INTEREST

There were no declarations of interest made.

0908. MINUTES OF THE STANDARDS COMMITTEE HELD ON 9 FEBRUARY 2017

Moved by Councillor H J Gilmour and seconded by Councillor C R Moesby.

RESOLVED that the Minutes of the meeting of the Standards Committee held on 9 February 2017 be approved as correct record.

0909. REVIEW OF THE COUNCIL'S CONSTITUTION

Members considered a report of the Assistant Director for Governance and Monitoring Officer confirming all the changes discussed at recent meetings of the Constitution Working Group.

Table 1 within the report set out the areas reviewed, whilst Appendix A went in to those areas in detail giving a rationale for each change. Appendix B set out each area of the Constitution in turn with tracked changes.

Members considered the proposed amendments to the Council's Constitution prior to submission as part of the annual review of the Constitution to Council for adoption. Members were happy with the content of the report but requested further consideration in regard to consistency with numbers and a review of the document for typographical errors.

Moved by Councillor B Watson and seconded by Councillor C Moesby.
RESOLVED that:-

(1) The amendments to the Constitution attached at **Appendix A** be recommended to Council for adoption.

(2) The areas of focus for the forthcoming 2017/18 review be noted.

(3) It be recommended to Council that delegated power be given to the Monitoring Officer to make changes to the Constitution arising from any new legislation, administrative errors or conflicts in the interpretation.

0910. COMPLAINTS OF BREACH OF THE CODE OF CONDUCT – 2017

The Standards Committee considered a report of the Assistant Director for Governance and Monitoring Officer which set out details of complaints of Breach of the Code of Conduct for the calendar year commencing January 2017. It was noted that one complaint had been received, which related to a Parish Council, and the Monitoring Officer's decision, in consultation with the Independent Persons, was that no further action should be taken.

Any further complaints that had been received were not applicable under the Code and therefore not reported.

Moved by Councillor C Moesby and seconded by Councillor B Watson.
RESOLVED that the Complaints of Breach of the Code of Conduct 2017 for Bolsover District Council be noted.

0911. WORK PLAN 2016/17

Members considered the Standards Committee Work Plan for 2016/17. The Chair requested for Members to let her know if they wished for any items to be included within her Annual Report to Council.

Moved by Councillor C Moesby and seconded by Councillor B Watson.
RESOLVED that the Work Plan 2016/17 be noted.

0912. PROPOSED WORK PLAN FOR 2017/18

The Standards Committee considered the Work Plan for 2017/18, which had been supplied to them in a different format to provide greater clarity. It was noted that the Work Plan indicated that the RIPA Review and the Review of the Member/Officer Protocol would be submitted to their forthcoming meeting on 4 June 2017.

Moved by Councillor C Moesby and seconded by Councillor B Watson.
RESOLVED that the Work Plan be noted.

0913. SUPPLEMENTARY REPORT ON THE DEFINITION OF "EXECUTIVE DECISION" FOR INCLUSION IN THE CONSTITUTION

Members received a supplementary report of the Assistant Director for Governance and Monitoring Officer providing Members with a definition of "Executive Decisions" for inclusion in the Council's Constitution.

As previously reported to the Constitution Working Group the practice has been to record every Executive Decision on a Delegated Decision form and then publish in accordance with statutory rules. The Constitution Working Group decided that there should be a definition of "Executive Decision" in the Constitution so that decisions outside that definition would not be placed on the website.

The Working Group were content that the financial figure for this should be £50,000. Members considered the wording suggested within the report.

Moved by Councillor B Watson and seconded by Councillor H J Gilmore.

RESOLVED that the following be added to paragraph 4.2.18 to the Access to Information Rules of the Constitution and that the rest of the paragraph is re-numbered accordingly:-

Executive Decision is defined as a decision in connection with the discharge of an Executive function, which will, or is likely to incur expenditure or savings in excess of £50,000 or generate a revenue return/income in excess of £50,000 as a specific consequence of that decision.

The meeting concluded at 1014 hours.

Agenda Item No 5

Bolsover District Council

Standards Committee

5th September 2017

Review of Protocol on Member/Officer Relations

Report of the Assistant Director – Governance and Solicitor to the Council & Monitoring Officer

This report is public

Purpose of the Report

- For Members to consider the Protocol on Member/Officer Relations

1 Report Details

1.1 Following the review of the Constitution in 2016/17, the Constitution Working Group considered that the Protocol on Member/Officer Relations would be a suitable focus for the review in 2017/18.

1.2 The Committee will consider a wider review of the Constitution as well during the year; however this report allows Members to focus on this Protocol in particular, as an opportunity for more targeted scrutiny.

1.3 The Council's Protocol on Member/Officer Relations is contained within Part 5 of the Constitution and is part of a suite of Codes and Protocols applying to Members and Officers. There is a dedicated Code of Conduct for Members and a separate one for Employees.

1.4 The purpose of the Protocol on Member/Officer Relations is to provide guidance to Members and Officers in their relations with one another. It is not a prescriptive or exhaustive set of rules, but provides guidance and principles to be followed to achieve the shared aim of enhancing and maintaining the integrity of local government through high standards of personal conduct.

1.5 At this stage, it is not envisaged that any major changes will be recommended to the Protocol or the ways in which Members and Officers interact, however some revisions may be suggested to make the text more accessible and the guidance easier to understand and follow.

2 Conclusions and Reasons for Recommendation

2.1 It is best practice that the Council's Constitution be reviewed on a regular basis and the Standards Committee has usually carried this out annually. It was agreed that the Protocol on Members/Officer Relations be the focus of this year's review.

2.2 Members are therefore asked to give their comments on the Protocol which Officers can take away to be included in the review that will be presented to a future meeting.

3 Consultation and Equality Impact

3.1 This report forms part of the process for Members to contribute to the review of the Constitution. The Senior Management Team will also be consulted as part of the review. It is not envisaged that there are any equalities issues arising from this review.

4 Alternative Options and Reasons for Rejection

4.1 The Committee could agree that the Protocol does not require further review or could suggest other areas of focus.

5 Implications

5.1 Finance and Risk Implications

5.1.1 None

5.2 Legal Implications including Data Protection

5.2.1 Any legal implications will be dealt with as part of the review.

5.3 Human Resources Implications

5.3.1 None

6 Recommendations

6.1 That Members consider the Protocol on Member/Officer Relations and make any comments arising from this to be included in the review.

7 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: *BDC: Revenue - £75,000* ☐ *Capital - £150,000* ☐ *NEDDC: Revenue - £100,000* ☐ *Capital - £250,000* ☐ ☑ *Please indicate which threshold applies*	Yes/No

Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	Yes/No
District Wards Affected	All
Links to Corporate Plan priorities or Policy Framework	All

8 Document Information

Appendix No	**Title**
Appendix 1	Protocol on Member/Officer Relations taken from the Council's Constitution
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 (NEDDC) or Executive (BDC) you must provide copies of the background papers)	
None	

Report Author	**Contact Number**
Donna Cairns, Governance Manager (Acting)	Ext 2505

5.3 PROTOCOL ON MEMBER/OFFICER RELATIONS

1. Introduction

(1) The purpose of this protocol is to guide Members and officers of the Council in their relations with one another.

(2) Given the variety and complexity of such relations, this protocol does not seek to be either prescriptive or comprehensive. It seeks simply to offer guidance on some of the issues which most commonly arise.

(3) This protocol also seeks to reflect the principles underlying the respective Codes of Conduct which apply to Members and officers. The shared aim of these codes is to enhance and maintain the integrity (real and perceived) of local government and they, therefore, demand very high standards of personal conduct.

(4) The Council's Code of Conduct for Members and the Code of Conduct for employees make it clear how the Members and Officers should treat each other:

2. Members and Officers

(1) Both Members and Officers are servants of the public, and they are indispensable to one another but their responsibilities are distinct. Members are responsible to the electorate and serve only so long as their term of office lasts. Officers are responsible to the Council. Their job is to give advice to Members and the Council, and to carry out the Council's work under the direction and control of the Council, its committees and sub-committees and the Executive.

(2) Members must not do or threaten to do anything which compromises or which is likely to compromise the impartiality of an employee of the Council.

(3) Mutual respect between Members and officers is essential to good local government. Close personal familiarity or hostility between individual Members and officers can damage this relationship and prove embarrassing to other Members and officers.

(4) The law and the Council's procedures lay down rules for the appointment, discipline and dismissal of staff. Members must ensure that they observe these scrupulously at all times. Special rules apply to the appointment of assistants to political groups. In all other circumstances, if a Member is called upon to take part in appointing an Officer, the only questions which the Member should consider is which candidate would best serve the whole Council. Members should not let their political or personal preferences influence their judgement. They should not canvass the support of colleagues for any candidate and should resist any attempt by others to canvass theirs. In consequence, Members should not provide references in support of applications for employment by the Council.

(5) In line with the Council's Codes' reference to "mutual respect", it is important that any dealings between Members and officers should observe reasonable standards of courtesy and that neither party should seek to take unfair advantage of their position or be hostile to the other.

(6) The Employee Code adopted by the Council has similar wording:

"Mutual respect between employees and councillors is essential to good local government. Close personal familiarity or hostility between employees and individual councillors can damage the relationship and prove embarrassing to other employees and councillors and should therefore be avoided."

3. Officer advice to Party Groups

(1) There is now statutory recognition for party groups and it is common practice for such groups to give preliminary consideration to matters of Council business in advance of such matters being considered by the relevant Council decision making body. Officers may properly be called upon to support and contribute to such deliberations by party groups.

(2) The support provided by officers can take many forms, ranging from a briefing meeting with a Chairperson or Spokesperson prior to a Committee meeting to a presentation to a full party group meeting. Whilst in practice such officer support is likely to be in most demand from whichever party group is for the time being in control of the Council, such support is available to all party groups.

(3) Certain points must, however, be clearly understood by all those participating in this type of process, Members and officers alike. In particular:

(a) Officer support in these circumstances must not extend beyond providing information and advice in relation to matters of Council business. Officers must not be involved in advising on matters of party business. The observance of this distinction will be assisted if Officers are not expected to be present at meetings, or parts of meetings, when matters of party business are to be discussed;

(b) Party group meetings, whilst they form part of the preliminaries to Council decision making, are not empowered to make decisions on behalf of the Council. Conclusions reached at such meetings do not, therefore, rank as Council decisions and it is essential that they are not interpreted or acted upon as such; and

(c) Similarly, where Officers provide information and advice to a party group meeting in relation to a matter of Council business, this cannot act as a substitute for providing all necessary information and advice to the relevant Committee or Sub-Committee when the matter in question is considered.

(4) Special care needs to be exercised whenever Officers are involved in providing information and advice to a party group meeting which includes persons who are not Members of the Council. Such persons will not be bound by the Council's Code of Conduct (in particular, the provisions concerning the declaration of interests and confidentiality) and for this and other reasons Officers may not be able to provide the same level of information and advice as they would to a Members only meeting.

(5) Officers must respect the confidentiality of any party group discussions at which they are present and should not relay the content of any such discussion to another party group.

(6) Any particular cases of difficulty or uncertainty in this area of officer advice to party groups should be raised with the Chief Executive who will discuss them with the relevant group leader(s).

4. Support Services to Members and Party Groups

The only basis on which the Council can lawfully provide support services (e.g. stationery, typing, printing, photo-copying, transport, etc.) to Members is to assist them in discharging their role as Members of the Council. Such support services must, therefore, only be used on Council business. They should never be used in connection with party political or campaigning activity or for private purposes.

5. Members' Access to Information and to Council Documents

(1) Members are free to approach any Director or Assistant Director, as appropriate, to provide them with such information, explanation and advice (about that Directorate or Service functions) as they may reasonably need in order to assist them in discharging their role as Members of the Council. This can range from a request for general information about some aspect of Directorate or service activities to a request for specific information on behalf of a constituent. There is no automatic right to such information, except in the circumstances outlined below where the "Need to Know" is established. Such approaches should normally be directed to the Director or Assistant Director.

(2) As regards the legal rights of Members to inspect Council documents, these are covered partly by statute and partly by common law.

(3) Members have a statutory right to inspect any Council document, which contains material relating to any business which is to be transacted at a Council, Committee or Sub-Committee or Executive meeting. This right applies irrespective of whether the Member is a Member of the Executive, a Committee or Sub-Committee concerned and extends not only to reports, which are to be submitted to the meeting, but also to any relevant background papers. This right does not, however, apply to documents relating to certain items which may appear on the "Exempt" part of the agenda for meetings. The items in question are those which contain exempt information relating to employees, occupiers of Council property, applicants for grants and other services, contract and industrial relations negotiations, advice from Counsel and criminal investigations.

(4) The common law right of Members is much broader and is based on the principle that any Member has a prima facie right to inspect Council documents so far as access to the document is reasonably necessary to enable the Member properly to perform their duties as a Member of the Council. This principle is commonly referred to as the "Need to Know" principle.

(5) The exercise of this common law right depends, therefore, upon the Member's ability to demonstrate the necessary "Need to Know". In this respect a Member has no right to "a roving commission" to go and examine documents of the Council. Mere curiosity is not sufficient. The crucial question is the determination of the "Need to Know". This question must initially be determined by the particular Director or Assistant Director as appropriate whose staff holds the document in question (with advice from the Monitoring Officer). It follows from this that the Member must give the reason for the enquiry. In the event of dispute, the question falls to be determined by the relevant Committee - i.e. the committee in connection with whose functions the document is held or the Executive.

(6) In some circumstances (e.g. a Committee Member wishing to inspect documents relating to the functions of that Committee) a Member's "Need to Know" will normally be presumed. In other circumstances (e.g. a Member wishing to inspect documents which contain personal information about third parties) a Member will normally be expected to justify the request in specific terms.

(7) Whilst the term "Council document" is very broad and includes, for example, any document produced with Council resources, it is accepted by convention that a Member of one party group will not have a "Need to Know", and, therefore, a right to inspect, a document which forms part of the internal workings of another party group.

(8) Further and more detailed advice regarding Members' rights to inspect Council documents may be obtained from the Assistant Director – Governance and Monitoring Officer.

(9) Finally, any Council information provided to a Member must only be used by the Member for the purpose for which it was provided, i.e. in connection with the proper performance of the Member's duties as a Member of the Council.

7. Officer/Chairperson Relationship

(1) It is clearly important that there should be a close working relationship between the Chairperson of a Committee or Member Working Group and the Director, Assistant Director and other senior Officers, which reports to that Committee or Member Working Group. However, such relationships *should never be allowed to become so close, or appear to be so close, as to bring into question the Officers' ability to deal impartially with other Members and other party groups*.

(2) In relation to action between meetings, it is important to remember that the law allows for decisions (relating to the discharge of any of the Council's functions) to be taken by a Committee, a Sub-Committee or an Officer and in relation to Executive functions by the Executive or an Officer. Legislation allows for Members to take individual decisions where the Council decides that this should happen. These decisions can only be taken in specific circumstances following appropriate advice and the decision must be recorded. This does not mean that any decision can be taken by a Member. The rules relating to decision making where it is a Committee or Sub Committee or Officer decision remain unchanged.

(3) The Council's delegation scheme is contained within the Constitution. This contains the majority of delegations to officers. From time to time the Executive, Committees and the Council give additional delegations which are added to the Constitution as it is updated annually.

(4) Finally, it must be remembered that Officers within any department are directly accountable to the Chief Executive Officer. Whilst Officers should always seek to assist a Chairperson (or indeed any Member), they must not, in so doing, go beyond the bounds of whatever authority they have been given by the Chief Executive Officer.

8. Correspondence

(1) Correspondence between an individual Member and an Officer should not normally be copied (by the Officer) to any other Member. Where exceptionally it is necessary to copy the correspondence to another Member, this should be made clear to the original Member. In other words, a system of "silent copies" should not be employed.

(2) Official letters on behalf of the Council should normally be sent out over the name of the appropriate officer, rather than over the name of a Member generally. It may be appropriate in certain circumstances (e.g. representations to a Government Minister) for a letter to appear over the name of a Member. Letters which, for example, create obligations or give instructions on behalf of the Council should never be sent out over the name of a Member.

Where Members send correspondence in their own name as a Member of the Council, such correspondence may be sent on Council headed notepaper headed with the words “from the Office of [Name of Councillor]”

9. Involvement of Ward Councillors

(1) Whenever a public meeting is organised by the Council to consider a local issue, all the Members representing the Ward or Wards affected should as a matter of course be invited to attend the meeting. Similarly, whenever the Council undertakes any form of consultative exercise on a local issue, the Ward Members should be notified at the outset of the exercise.

10. When and how Members can access information from data systems.

(1) On occasion elected members require personal customer data (as defined by the Date Protection Act) to carry out their duties, for example for declaring interests on Licensing Committee or considering objections at Planning Committee. Usually this data is presented to elected members in a format which protects the original data.

(2) Elected members should not have direct access to systems which control or process personal data; unless it is contained in a public register. Elected members do though have the right (whether or not they have a personal data protection registration) to view data which enables them to carry out their duties e.g. viewing a collated list of personal data submitted as part of a licensing function.

(3) With regard to CCTV, an authorised list of users has been established. The authorised users include Police Officers (which are covered in the legislation) and employees of the Council who need access to carry out their operational duties as defined in their job description. The system should only be accessed for a specific purpose by specific authorised people. The Council has a duty to ensure all data is fully protected at all times.

(4) On some occasions it is appropriate for elected members, third parties and senior officers to 'view' CCTV data. This is documented in the CCTV Code. If someone in a senior position wanted to view (not access or operate) the CCTV they must have a valid reason e.g. major incident in Bolsover Market Place between 1.00 - 2.00 am on Sunday. They would not be given a password or allowed to operate the system themselves. They would have to sign the viewing confidentiality declaration and viewing log. This is designed to remove any security risk for the person and the Authority. By completing this documentation the senior officer or elected member can then sit with the authorised person and 'view' the data on the screen. The authorised person controls the system and viewing at all times to ensure privacy is maintained for people and houses in the vicinity of the cameras. This is detailed in the Code.

Agenda Item No 6

Bolsover District Council

Standards Committee

5th September 2017

Review of Joint RIPA Policy

Report of the Assistant Director of Governance and Solicitor to the Council and Monitoring Officer

This report is public

Purpose of the Report

- To advise the Committee of a review of the joint policy and procedures covering the Council's activities under the Regulation of Investigatory Powers Act 2000 (RIPA).

- To recommend minor amendments to the Joint RIPA Corporate Policy and Procedures.

1 Report Details

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

1.2 Local authorities are sparing users of RIPA legislation and neither Bolsover nor North East Derbyshire District Councils have used them in the last four years. Officers within the Benefits section have assisted the Department of Work and Pensions - who are not required to obtain judicial approval - on applications and investigations.

1.3 The Councils' use of RIPA is also subject to inspection by the Surveillance Commissioner. The last inspection that was carried out by the Assistant Surveillance Commission, took place in November 2015. The Assistant Commissioner concluded that although the powers had not been used since the previous inspection, the procedures and the level of awareness in place were sufficient to ensure future applications would be compliant with the Act. The limited recommendations that were made included minor amendments to the policy, including reference to social media (para 4.7) and the current Joint Policy and Procedures document was amended in 2015/16 in line with these

recommendations. A further recommendation focused on ensuring a good level of awareness of the policy across Councillors through regular reporting.

1.4 This report serves to provide Members with an update on the usage of the RIPA powers and to allow the opportunity for Members to have oversight of the policy and procedures. As mentioned above, the RIPA powers have not been used since the last report to Standards Committee in December 2015.

1.5 There have been no changes in the regulations since the last review and the previous Code of Practice issued in 2014 is still current. Reports on recent inspections of other local authorities have been considered, as well as recent rulings of the Investigatory Powers Tribunal.

1.6 No significant changes are proposed following this review of the Joint Policy and Procedures, however the changes in the Strategic Alliance Management Team structure has required that alternative arrangements be made to the 'authorising officers' and 'designated persons' named within the policy. As the Councils' Senior Responsible Officer, responsible for appointing 'authorising officers' and 'designated persons', the Monitoring Officer has proposed appointing the Assistant Director – Finance and Revenues and Benefits, having removed the Executive Director – Operations and the Executive Director – Transformation from the policy.

1.7 Further changes may be made to these appointments later in the year. It is proposed that the policy be updated by the Monitoring Officer to reflect these appointments made from time to time, without requiring the document to be brought back to this Committee and Executive for approval. An annual report would still be brought to Standards Committee with an update on the usage of the RIPA powers and on any changes to appointments to persons as 'authorising officers' and 'designated persons'.

1.8 The Councils previously had a protocol attached to the policy for working with the local Magistrates Court on the processing of applications under RIPA. This has been removed from the Policy as the protocol included information on the workings of the Magistrates Court that needs to be controlled, however the arrangements for working efficiently with the Court remain in place. The protocol is held by the Governance Team who will provide a copy to any applicant and authorising officer seeking approval from the Magistrates Court.

1.9 The only other amendments to the policy are intended to reflect staffing changes and minor clarifications.

1.10 If supported by the Standards Committee the recommended amendments to the policy and procedures document will be reported to the next meeting of the Strategic Alliance Joint Committee before being submitted to the Executive for approval.

1.11 To ensure that the Council is undertaking investigatory activity in compliance with the law and this policy, refresher training is provided regularly for all relevant officers. Further training will be provided later in 2017 and will be available for officers to refer to on the Councils' intranet sites.

2 Conclusions and Reasons for Recommendation

2.1 No changes have been made in the relevant legislation and codes of practice therefore the purpose of the amendments are to ensure the policy remains accurate and up-to-date.

3 Consultation and Equality Impact

3.1 An Equality Impact Assessment has been completed, which concluded that there were no concerns raised and no actions to take.

4 Alternative Options and Reasons for Rejection

4.1 The Council is recommended to review and update its RIPA policy regularly as failure to do so could result in the policy failing to comply with legislative changes and lead to unlawful investigatory actions taking place.

5 Implications

5.1 Finance and Risk Implications

5.1.1 Failure of the Council to adhere to the legal requirements of RIPA could lead to unlawful investigatory activity being undertaken, making the Council vulnerable to complaints, legal challenge and reputational damage. It is important therefore that the policy is regularly reviewed and that officers receive sufficient training which will mitigate the likelihood of this risk occurring.

5.2 Legal Implications including Data Protection

5.2.1 The legal implications are addressed within the policy.

5.3 Human Resources Implications

5.3.1 None arising from this policy.

6 Recommendations

6.1 That Standards Committee:

(1) note the update provided on the use of the policy.

(2) consider and comment on the revised Joint Policy and Procedure document

(3) subject to any comments made by the Committee, recommend the revised Joint RIPA Policy and Procedure document for approval.

(4) recommend that the Joint RIPA Policy and Procedures document be updated by the Monitoring Officer to reflect the appointment of Authorised Officers and Designated Persons, made by the Monitoring Officer at any future time.

7 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: *BDC: Revenue - £75,000* ☐ *Capital - £150,000* ☐ *NEDDC: Revenue - £100,000* ☐ *Capital - £250,000* ☐ ☑ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
District Wards Affected	All
Links to Corporate Plan priorities or Policy Framework	All

8 Document Information

Appendix No	**Title**
1	Joint RIPA Policy and Procedures
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 (NEDDC) or Executive (BDC) you must provide copies of the background papers)	

Report Author	**Contact Number**
Donna Cairns, Governance Manager (Acting)	01246 217753

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

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	First draft
Policy author	~~M Kane~~ Governance Manager
Location of policy – i.e. L-drive, shared drive	~~L~~ S Drive
Member route for approval	Strategic Alliance Joint Committee and Standards
Cabinet Member (if applicable)	Cllrs K Reid and N Barker
Equality Impact Assessment approval date	July 2017 ~~N/A~~
Partnership involvement (if applicable)	N/A
Final policy approval route i.e. Executive/ Council /Planning Committee	Cabinet / Executive
Date policy approved	
Date policy due for review (maximum three years)	Autumn 2018
Date policy forwarded to Strategy and Performance (to include on Intranet and Internet if applicable to the public)	

Contents

10. Training and Advice and Departmental Policies, Procedures and Codes of Conduct
    - 10.1 Training and Advice
    - 10.2 Departmental Policies, Procedures and Codes of Conduct

11. Complaints

12. Monitoring of Authorisations

1. Abbreviations

CCTV	Closed Circuit Television
CSP	Communications service provider
Council	Bolsover/North East Derbyshire District Council
CHIS	Covert Human Intelligence Sources
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedom agreed on 2 November 1950
HRA	Human Rights Act 1998
ICCO	The Interception of Communications Commissioner's Office
NAFN	The National Anti Fraud Network
OSC	Office of Surveillance Commissioners
PFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SPoC's	Single Points of Contact for Acquisition and Disclosure of Communications Data

Introduction

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.

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.

Any potential use of RIPA should be referred to the Monitoring Officer, Sarah Sternberg, for preliminary advice at the earliest possible opportunity. Her telephone number is 01246 ~~217058/~~242414. In her absence, advice should be sought from ~~her deputies Adele Wylie (BDC) and Matthew Kane (BDC/NEDDC~~ the Governance Team on 01246 217753). ~~Their phone numbers are 01246 242477 (AW) and 01246 217753/242505/0799 9924276 (MK).~~

Consequences of Failing to Comply with this Policy

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 will be inadmissible.

2. Background

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

The ECHR states:-

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

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

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

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 might otherwise breach the ECHR. These activities are:-

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

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.

A flow chart attached at **Appendix A** to this policy sets out the process in pictorial form.

What RIPA Does and Does Not Do

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.

RIPA does not:-

- make unlawful conduct with 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.

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.

3. Policy Statement

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, Bolsover and North East Derbyshire District Council adopted separate RIPA Policies in 2013, which have subsequently been combined into a single Corporate Policy and Procedures document as detailed below.

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 4.6 (in respect of handling confidential information) and 5.2 (in respect of using information sources who are vulnerable or juvenile persons) below.

The following documents are available on the Council's intranet:-

- 2014/15 Home Office Statutory Codes of Practice on:-

    - Covert Surveillance and Property Interference
    - Covert Human Intelligence Sources
    - Acquisition and Disclosure of Communications Data

- Office of the Surveillance Commissioners' Guidance Procedures
- Home Office Guidance on Protection of Freedoms Act 2012 – changes to RIPA;
- RIPA forms for covert surveillance; CHIS and acquisition and disclosure of communications data;
- Application for Judicial approval and Order made for Judicial approval;
- Surveillance camera training;
- Corporate RIPA Training.

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

- Appointing Authorising Officers (see 8.1[a]);

- Appointing Designated Persons (see 8.1[a]);
- Maintaining a central record for all RIPA authorisations;
- Arranging training to individuals appointed as Authorising Officers and Designated Persons, and
- Carrying out an overall monitoring function as the SRO for the Council's use of RIPA powers.

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

4. Types of Surveillance

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.

4.1 Overt Surveillance

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.

4.2 Covert Surveillance

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 4.3 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 4.4 below explains when covert surveillance is directed.

4.3 Covert intrusive Surveillance

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.

4.4 Covert Directed Surveillance

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, home and correspondence (whether at home, in a public place or in the work place).

4.5 Directed Surveillance Crime Threshold

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.

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.

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

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

4.6 Confidential Information

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).

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 Chief Executive or in their absence by an officer acting as Head of Paid Service**.

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.

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.

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

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

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

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

4.7 Social Media

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. 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, including the effect of any collateral intrusion. Advice should be sought.

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

5. Covert Human Intelligence Sources ("CHIS")

5.1 CHIS

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

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

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

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

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".

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 attendance and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

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.

The Home Office Statutory CHIS Code of Practice can be found on the Home Office website and on the intranet.

5.2 Vulnerable Individuals/Juvenile CHIS

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.

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 Chief Executive or in their absence by an officer acting as 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.**

The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them.

In other cases authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. This set out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

6. CCTV

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 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.

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.

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.

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

7. Acquisition and Disclosure of Communications Data

7.1 Communication Service Providers ("CSPs")

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.

7.2 Types of Communications Data

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

Service Use Information

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

Subscriber information

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

Traffic Information

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.**

7.3 Authorisation and Notices

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

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

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

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

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

As a local authority the Council must fulfil two additional requirements when acquiring communications data. Firstly, the request must be made through a SPoC at NAFA (see more about NAFA at 8.3(b) and 8.4). Secondly, the request must receive prior judicial approval.

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

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

8 Authorisation Procedures

Authorisations given by Authorising Officers and Designated Persons are subject to approval by the Magistrates Court (See para 8.3 below)

8.1 (a) Authorising Officers/Designated Persons be directed surveillance and CHIS

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

Designated Persons fulfil a similar role in relation to applications to obtaining communications data, assessing and approving authorisations and notices.

It is the responsibility of Authorising Officers and Designated Persons to ensure that when applying for authorisation the principles of necessity and proportionality (see 8.2 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (8.8 – 8.10 below).

Lists of authorising officers and designated persons are set out below. Any requests for amendments to the lists must be sent to the Monitoring Officer.

The authorising officers and designated persons for Bolsover and North East Derbyshire District Councils are as follows:

Chief Executive – Dan Swaine (01246 242401/217155)
Assistant Director – Finance and Revenues and Benefits – Dawn Clark (01246 217658)
~~Executive Director – Operations – Bryan Mason (01246 242431/217053)~~
~~Executive Director – Transformation – Paul Hackett (01246 242566/217543)~~

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

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

8.1(b) Single Point of Contact (SPoC)

SPoCs are responsible for advising officers within the Council on how best to go about obtaining communications data, for liaising with CSPs, and advising whether applications and notices are lawful. As required under the latest Acquisition and Disclosure of Communications Data Code of Practice, the Council has engaged the National Anti-Fraud Network (NAFN). NAFN's SPoC services relate only to communications data. For information on using NAFA, see 8.4 below.

8.2 Authorisation of Covert Directed Surveillance and Use of a CHIS

RIPA applies to all covert directed surveillance, use of CHIS and acquisition and disclosure of communications data 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 (see para 8.6) authorising officer. Authorisations or notices in relation to communications data should be referred to NAFN.

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

Covert directed surveillance, use of a CHIS and acquisition and disclosure of communications data can only be authorised if the authorising officer/designated person is satisfied that the activity is:-

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

(b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and there is a crime threshold for directed surveillance as described in paragraph 4.5 above; and

(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.

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.

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

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/designated person, particularly when considering the proportionality of the surveillance.

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

The activity must be authorised, including approval by the Magistrates Court before it takes place.

At the time of authorisation the authorising officer/designated person must set a date for review of the authorisation and review it on that date (see 8.8), prior to authorisation lapsing.as it must not be allowed to lapse.

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

8.3 Approval by Magistrates Court

Following changes under the Protection of Freedoms Act 2012, there is now an additional stage in the process for all three investigatory activities (covert directed surveillance, CHIS

and Communications Data). After the authorisation form has been countersigned by the authorising officer/designated person, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

The Council has a protocol for the Magistrates' approval process, which is held by the Governance Team. ~~attached as **Appendix B**.~~

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

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.

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

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.**

The Role of the Magistrates Court

The role of the Magistrates Court is set out in Section 23A RIPA (for communications data) and Section 32A RIPA (for directed surveillance and CHIS).

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

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

- 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 or designated person (as appropriate);

- The grant of the authorisation or, in the case of communications data, notice was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
  - 25(3) (for communications data),
  - 29(7)(a) (for CHIS),
  - 30(3) (for directed surveillance and CHIS).

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

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

8.~~3~~4 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.

8.~~4~~5 Authorisation of Acquisition and Disclosure of Communications Data

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

- Applicant
- Designated Person
- Single Point of Contact

Applicant

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

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

Designated Person

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

Single Point of Contract (SPoC)

The accredited SPoCs at NAFN scrutinise the applications independently, and provide advice to applicant officers and designated persons ensuring the Council acts in an informed and lawful manner.

The procedure for applying for acquisition of communications data:

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

8.~~5~~6 Urgent Authorisations

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.

8.~~6~~7 Application Forms

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

(c) Acquisition and Disclosure of Communications Data

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

8.~~7~~ 8 Duration of the Authorisation

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 value for 12 months after the date of authorisation (or after one month if a juvenile CHIS is issued);
- a communications data notice remains valid for a maximum of one month.

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

8.~~8~~9 Review of Authorisations

As referred to at 8.2 authorising officers/designated persons must make arrangements to periodically review any authorised RIPA activity. Officers carrying out RIPA activity, or external agencies engaged by the Council to carry out RIPA activity, must periodically review it and report back to the authorising officer/designated person if there is any doubt

as to whether it should continue. Reviews should be recorded on the appropriate Home Office Form (see 8.6).

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.

8.~~9~~10 Renewal of Authorisations

If the authorising officer/designated person considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained. Renewed authorisations will normally be for a period of up to three months for covert directed surveillance, 12 months in the case of CHIS, one month in the case of juvenile CHIS and one month in the case of a communications data authorisation or notice. Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation. Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form (see 8.6). The reasoning for seeking renewal of a communications data authorisation or RIPA notice should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

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

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 Governance Team together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

8.~~10~~11 Cancellation of Authorisations

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

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.

8.~~11~~12 What happens if the surveillance has unexpected results?

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.

9. Records and Documentation

9.1 Departmental Records

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.

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

9.2 Central Record of Authorisations, Renewals, Reviews and Cancellations

A joint central record of directed surveillance, CHIS and access to communications data authorisations is maintained by the Monitoring Officer at the District Council Offices, Mill Lane, Wingerworth for both Bolsover and North East Derbyshire District Councils.

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/designated persons 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 8.2) send notification of every renewal, cancellation and review on the Council's notification forms (see 8.9 – 8.11).

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

- remind authorising officers/designated persons 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/designated persons 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.

9.3 Surveillance products and communications data

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.

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

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.

Material obtained through the use of directed surveillance, CHIS or acquisition of communications data containing personal information will be protected by the Data Protection Act 1998 (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.

10. Training & Advice and Departmental Policies, Procedures and Codes of Conduct

10.1 Training & Advice

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.

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

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

10.2 Departmental Policies, Procedures and Codes of Conduct

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.

11. Complaints

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

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

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

12. Monitoring of Authorisations

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

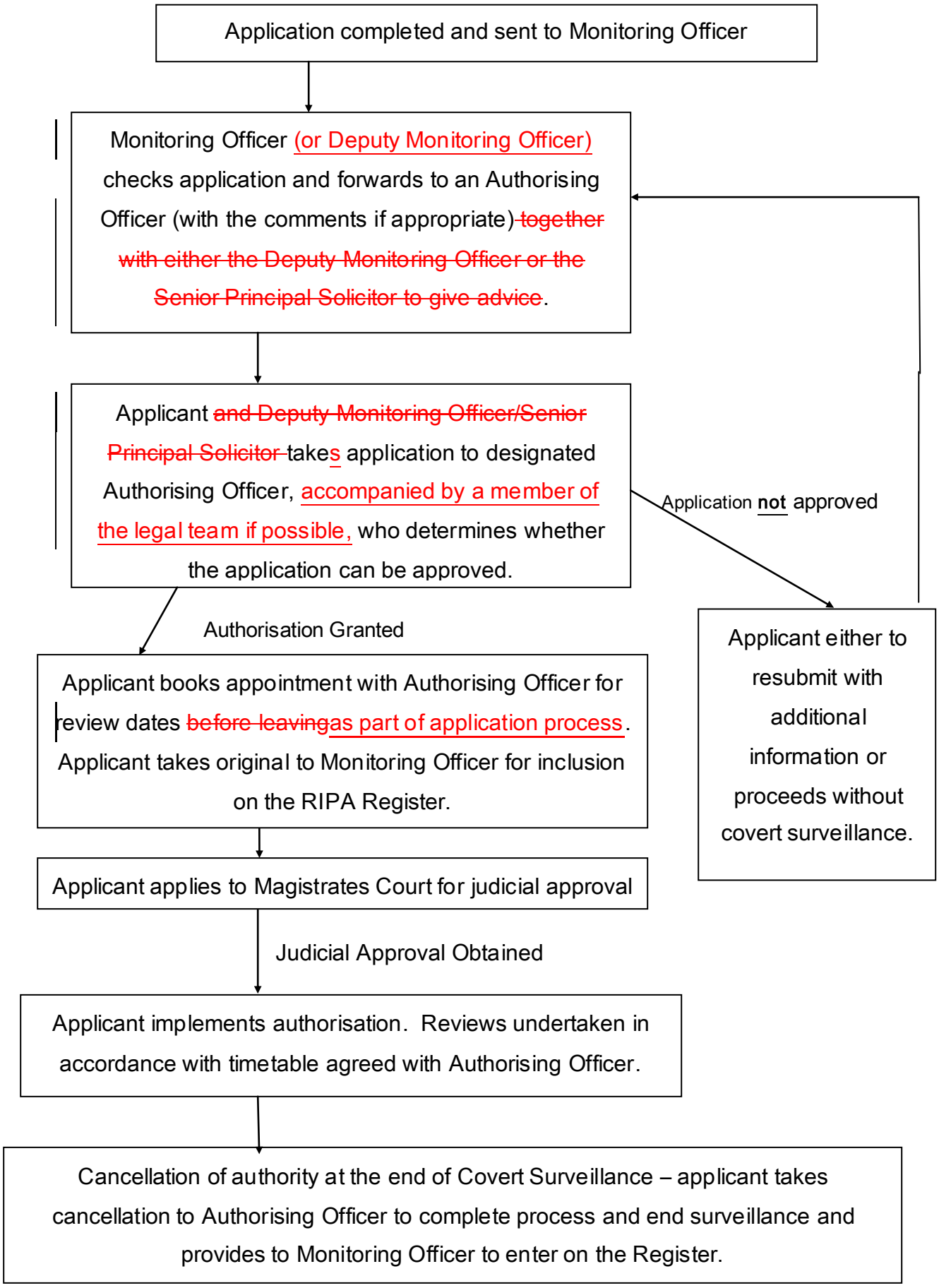
- The integrity of the process in place to authorise directed surveillance, the use of CHIS and the acquisition and disclosure of communications data;

- Compliance with Part II of RIPA and this Policy;
- Engagement with the Commissioners of the OSC and ICCO when they conduct inspections; and
- Where necessary, overseeing the implementation of any post-inspection plans recommended or approved by a Commissioner.

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.

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.

APPENDIX A - RIPA PROCESS



Agenda Item No 9

Bolsover District Council

Standards Committee

5 September 2017

Work Plan 2017/18

Report of the Assistant Director of Governance and Solicitor to the Council and Monitoring Officer

This report is public

Purpose of the Report

- To advise the Committee of its Work Plan for 2017/18.

1. Report Details

1.1 A copy of the Committee's current work plan for 2017/18 is attached as **Appendix 1** to this report.

1.2 The Parliamentary Committee on Standards in Public Life recently announced that it would be conducting a review of Local Government Standards, which would include a consultation exercise in early 2018. This has been added to the Work Plan for February 2018 but the report will depend on the timetable of the review.

1.3 The Committee is also asked to consider whether to set up another Constitution Working Group to assist with the review of the Constitution for this municipal year and to determine its membership, if required.

2 Conclusions and Reasons for Recommendation

2.1 To advise the Committee of the proposed work plan for 2017/18.

3 Consultation and Equality Impact

3.1 Not applicable.

4 Alternative Options and Reasons for Rejection

4.1 Not applicable.

5 Implications

5.1 Not applicable.

6 Recommendations

6.1 That the Committee considers the Work Plan for 2017/18.

6.2 That the Committee consider setting up a Constitution Working Group for 2017/18.

7 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: *BDC: Revenue - £75,000* ☐ *Capital - £150,000* ☐ *NEDDC: Revenue - £100,000* ☐ *Capital - £250,000* ☐ ☑ *Please indicate which threshold applies*	No
Is the decision subject to Call-In? (Only Key Decisions are subject to Call-In)	No
District Wards Affected	All
Links to Corporate Plan priorities or Policy Framework	Demonstrating good governance

8 Document Information

Appendix No	**Title**
1	Standards Committee Work Plan 2017/18

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 (NEDDC) or Executive (BDC) you must provide copies of the background papers)
N/A

Report Author	**Contact Number**
Donna Cairns Governance Manager (Acting)	01246 242505

BDC STANDARDS COMMITTEE WORK PROGRAMME 2017/18		
Meeting date	**Item**	**Comments**
12 June 2017	RIPA review – annual review Review of the Member/Officer Protocol Regular items - review of training needs for District and Parish Councillors, complaints update and work programme	Meeting was cancelled so agenda items added to next meeting.
5 September 2017	Review of the Member/Officer Protocol RIPA review – annual review Update on Recruitment of Independent Person Regular items - review of training needs for District and Parish Councillors, complaints update and work programme	
27 November 2017	Review of whistle blowing policy Annual review of Gifts and Hospitality Review of the Member/Officer Protocol Regular items - review of training needs for District and Parish Councillors, complaints update and work programme	
26 February 2018	Annual review of the Constitution Parliamentary Committee on Standards in Public Life - Review of Local Government Standards Regular items - review of training needs for District and Parish Councillors, complaints update and work programme	

8 May 2018	Annual review of the Constitution Annual report to Council by Chairman of Standards Committee Development of the Annual Standards Committee Work plan for the next year. Regular items - review of training needs for District and Parish Councillors, complaints update and work programme	