

# EXTRAORDINARY STANDARDS COMMITTEE

## AGENDA

*Thursday 7<sup>th</sup> January 2016 at 1400 hours, in Chamber Suite 1, The Arc, Clowne*

Item No.		Page No.(s)
	<b>PART 1 – OPEN ITEMS</b>	
1.	<b><u>Apologies for absence</u></b>	
3.	<b><u>Declarations of Interest</u></b>	
	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 matters arising out of those items	
	and if appropriate, withdraw from the meeting at the relevant time.	
4.	Recommendation from Executive held on 7 <sup>th</sup> September 2015; Public Space Protection Orders (PSPO).	3 to 5
5.	RIPA Policy.	6 to 36
6.	Ethical Standards for Providers of Public Services – Guidance.	37 to 62
7.	Complaints Against Members.	63 to 64
8.	Standards Committee Work Plan.	65 to 66

**Bolsover District Council**

**Extraordinary Standards Committee**

**7<sup>th</sup> January 2016**

**Public Space Protection Orders**

**Report of the Assistant Director Governance**

This report is public

**Purpose of the Report**

To ask Committee to amend the Council's delegation scheme within the Constitution to enable the Chief Executive Officer to decide whether Public Space Protection Orders may be made.

**1 Report Details**

On the 7<sup>th</sup> September the Executive resolved to make two Public Space Protection Orders (PSPOs) under section 59 of the Anti-social Behaviour Crime and Policing Act 2014 (the Act). The Executive also resolved

That Standards Committee be recommended to amend the Officer Delegation Scheme to enable the Chief Executive Officer to authorise the making of Public Space Protection Orders under Part 4 of the Anti-social Behaviour, Crime and Policing Act 2014

In order to make a decision Standards Committee will require a brief background to the new powers which were introduced by the Act.

PSPOs are orders that impose conditions on an area in order to address a particular problem that is or is likely become detrimental to the local community's quality of life. They replace powers to make Dog Control Orders (the power to place restriction on dogs and their owners), Designated Public Place Orders (the power to restrict drinking in public spaces) and Gating Orders (the power to restrict access to public highways). The new power is far wider than the powers that it replaces and can potentially be used to control any anti-social activity. For example the recently made Shirebrook and Langwith PSPO has the following restrictions

1. No consumption of alcohol
2. No unsealed vessels containing alcohol
3. No urinating
4. No littering
5. Not to congregate in groups of two or more persons within the alleyways which lead to Shirebrook Market Place.

Not all of these restrictions could have been imposed by the old powers.

Due to their broad nature and versatility the new powers are akin to byelaws, however, they are far less bureaucratic than both by law procedure and the powers they replace.

There are a number of legal requirements that need to be satisfied. Section 59 of the Act requires that before a local authority makes a PSPO it must be satisfied on reasonable grounds that two conditions are met. The first condition is that either: (a) activities carried on in a public place within the authority's area have had a detrimental effect on the quality of life of those in the locality, or (b) it is likely that activities will be carried on in a public place within that area and that they will have such an effect. The second condition is that the effect, or likely effect, of the activities: (a) is, or is likely to be, of a persistent or continuing nature, (b) is, or is likely to be, such as to make the activities unreasonable, and (c) justifies the restrictions by the notice.

Orders last for 3 years however they may be extended.

A breach of an order is a criminal offence and could result in a fixed penalty notice of up to £100 or on conviction a fine of £1000.

In addition due to the affect these orders will have on an area, officers consider that the Chief Executive Officer should first consult with the Leader or Deputy Leader before making a decision. Further in order to be effective there should be the power to incur costs of making, managing and revoking the order. The recommendation below reflects this.

Also the Chief Executive officer currently has power to make alcohol exclusions zones. As alcohol exclusion zones (designated public place orders) have been superseded by PSPOs this power should be removed from the delegation scheme.

## **2 Conclusions and Reasons for Recommendation**

The Executive is satisfied that the decision to make a PSPO can be made by an individual as opposed to the Executive. By granting the power to the Chief Executive Officer the decision making process is simplified.

## **3 Consultation and Equality Impact**

Not applicable

## **4 Alternative Options and Reasons for Rejection**

For the Executive to continue to determine whether to make PSPOs. The Executive is satisfied that such decisions can be made by the Chief Executive Officer

## **5 Implications**

### **5.1 Finance and Risk Implications**

None

## 5.2 Legal Implications including Data Protection

As contained in the report

## 5.3 Human Resources Implications

None

## 6 Recommendations

That Standards Committee recommend to Council that

- (1) the Officer Delegation Scheme is amended to enable the Chief Executive Officer to authorise the making of Public Space Protection Orders under Part 4 of the Anti-social Behaviour, Crime and Policing Act 2014 in consultation with the Leader or Deputy Leader of the Council and incur necessary expenditure to create, manage or revoke Public Space Protection Orders;
- (2) Paragraph 10.26 of the existing Scheme of Delegation for Officers (authorisation of alcohol exclusion zones) be removed

## 7 Decision Information

<b>Is the decision a Key Decision?</b> (A Key Decision is one which results in income or expenditure to the Council of £50,000 or more or which has a significant impact on two or more District wards)	No
<b>District Wards Affected</b>	
<b>Links to Corporate Plan priorities or Policy Framework</b>	

## 8 Document Information

Appendix No	Title
<b>Background Papers</b> (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)	
<b>Report Author</b>	<b>Contact Number</b>
Jim Fieldsend	01246 242472

Report Reference –

**Bolsover District Council**

**Extraordinary Standards Committee**

**7<sup>th</sup> January 2016**

**RIPA Corporate Policies and Procedures**

**Report of the Assistant Director – Governance and Monitoring Officer**

This report is public

**Purpose of the Report**

- To present a new joint policy and procedures document covering the Council's activities under the Regulation of Investigatory Powers Act 2000.

**1 Report Details**

- 1.1 The Regulation of Investigatory Powers Act 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.
- 1.2 Local authorities are sparing users of RIPA legislation. This has become more so since the enactment of the Protection of the Freedoms Act in 2012 which required local authority use of RIPA to be subject to approval by a Magistrate. Use of directed surveillance is also subject to a separate "seriousness threshold" which means that it may only be used where the offence is punishable by a maximum term of at least six months imprisonment, or where it would constitute an offence involving sale of tobacco or alcohol to underage children regardless of length of prison term.
- 1.3 In the past three years, neither Bolsover nor North East Derbyshire District Councils have used RIPA although 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. The Councils have also met with the Clerk to the Magistrates' Court to establish lines of communication and a procedure should the need to use RIPA arise.
- 1.4 Regardless of our low level of use, the Council is required to have in place up-to-date policies and procedures. Following the issue of new codes of practice for covert surveillance and CHIS in December 2014 and for acquisition, disclosure and retention of communications data in May 2015 a new joint policy covering the

Alliance has been produced and is attached for consideration. This will replace the separate policies each Council adopted in 2013.

1.5 The policies have been informed by a recent inspection from the Assistant Surveillance Commissioner on 17 November 2015. Feedback from the inspection was positive although a final report is still awaited.

1.6 Subject to discussions at Standards, this report will go forward to Cabinet/Executive in February 2016.

## **2 Conclusions and Reasons for Recommendation**

2.1 To ensure the Councils have in place a fit for purpose policy and procedures document that complies with legislation.

## **3 Consultation and Equality Impact**

3.1 None.

## **4 Alternative Options and Reasons for Rejection**

4.1 None.

## **5 Implications**

5.1 None.

## **6 Recommendations**

6.1 That Standards Committee notes the report and recommends the policy to Executive for adoption.

6.2 That Standards Committee provide any comments on the attached joint policy.

## **7 Decision Information**

<b>Is the decision a Key Decision?</b> (A Key Decision is one which results in income or expenditure to the Council of £50,000 or more or which has a significant impact on two or more District wards)	No
<b>District Wards Affected</b>	
<b>Links to Corporate Plan priorities or Policy Framework</b>	

## Document Information

<b>Appendix No</b>	<b>Title</b>
A	RIPA Corporate Policy and Procedures Document (Draft)
<b>Background Papers</b> (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	
<b>Report Author</b>	<b>Contact Number</b>
M Kane	7753

AGIN 4(d) (STANDS 1209) RIPA/AJD

# **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**

<b>Policy Details</b>	<b>Comments / Confirmation (To be updated as the document progresses)</b>
Policy title	RIPA Corporate Policy and Procedures
Current status – i.e. first draft, version 2 or final version	First draft
Policy author	M Kane
Location of policy – i.e. L-drive, shared drive	L 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	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)	
Date policy forwarded to Strategy and Performance (to include on Intranet and Internet if applicable to the public)	

## Contents

## Page

1. Abbreviations
2. Background
3. Policy Statement
4. Types of Surveillance
  - 4.1 Overt Surveillance
  - 4.2 Covert Surveillance
  - 4.3 Covert Intrusive Surveillance
  - 4.4 Covert Directed Surveillance
  - 4.5 Directed Surveillance Crime Threshold
  - 4.6 Confidential Information
5. Covert Human Intelligence Sources (“CHIS”)
  - 5.1 CHIS
  - 5.2 Vulnerable Adults/Juveniles CHIS
6. CCTV
7. Acquisition and Disclosure of Communications Data
  - 7.1 Communication Service Providers
  - 7.2 Types of Communication Data
  - 7.3 Authorisation and Notice
8. Authorisation Procedure
  - 8.1(a) Authorising Officers and Designated Persons
  - 8.1(b) Single Point of Contact (SPoC)
  - 8.2 Authorisation of Covert Directed Surveillance, Use of CHIS and Acquisition and Disclosure of Communications Data
  - 8.3 Additional Requirements for Authorisation of a CHIS
  - 8.4 Additional Requirements for the Authorisation of Acquisition and Disclosure of Communications Data
  - 8.5 Urgent Authorisations
  - 8.6 Application Forms
  - 8.7 Duration of the Authorisation
  - 8.8 Review of Authorisations
  - 8.9 Renewal of Authorisations
  - 8.10 Cancellation of Authorisations
  - 8.11 What happens if the surveillance has unexpected results?
9. Records and Documentation
  - 9.1 Departmental Records
  - 9.2 Central Record of Authorisations, Renewals, Reviews and Cancellations
  - 9.3 Surveillance products and communications data

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.

## 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.

**All uses 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). Their phone numbers are 01246 242477 (AW) and 01246 217753/242505 (MK).**

## 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 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.

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
- 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<sup>1</sup> 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 of 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.

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.

## 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**

### **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  
Executive Director – Operations – Bryan Mason  
Executive Director – Transformation – Paul Hackett

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 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).

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.

### **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, 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. **It is advisable that both the authorising officer and a member of the Legal Team attend the Magistrates to present the application.**

### **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 Authorising Officer proceeds to court;
- 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 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 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 DP proceeds to court;
- 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 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 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 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 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 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 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 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 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:-

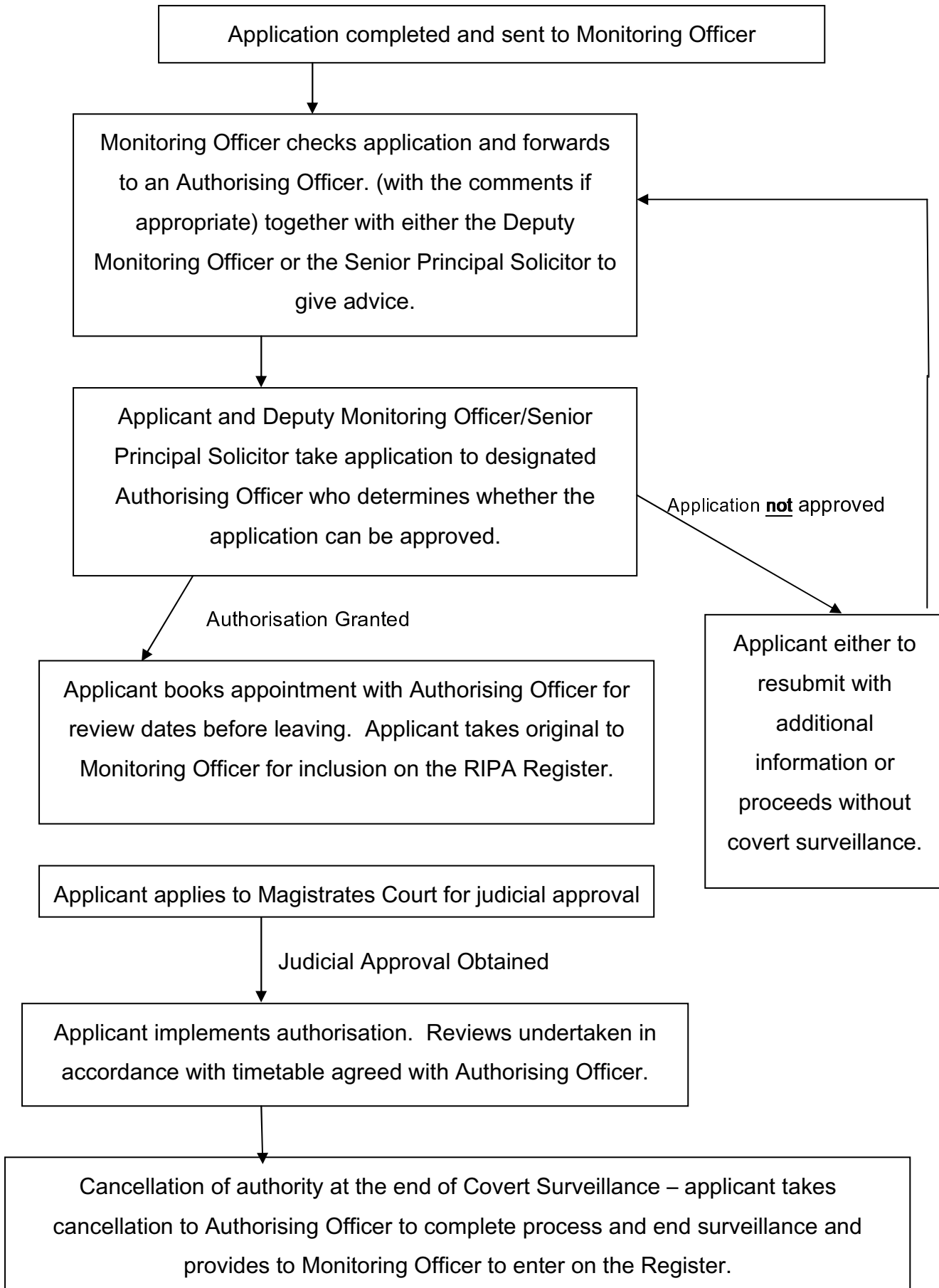
- The integrity of the process in place to authorise directed surveillance, the use of CHIS and the acquisition and disclosure of communications data;

- 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





## **APPENDIX B - RIPA applications process for Derbyshire Magistrates Court- non-police applicants**

### **Urgent application (for service within next 24 hours)**

- Applicant telephones the court of application (see below for contact details) to agree the time when the application can be made.
- Admin will contact the duty Clerk or available Legal Advisor (LA) to agree a suitable time and venue. Buxton – if no Legal Advisors available the applicant will be instructed to contact Chesterfield Court.
- Having agreed a time and venue for the application to be made the applicant will email the information and application to the relevant court generic email account. The Subject of the email must read 'Urgent or Non urgent application. The section under which the application is being made and if known the date of the application'.

### **Non urgent application**

- Applicant will email the Information, application and completed pro-forma to the court of application. Note: non availability of the applicant must be recorded to ensure accurate listing.
- Admin will email the pro-forma to the Duty Clerk or available LA for consideration and guidance on listing. The Subject of the email must read 'Urgent or Non urgent application. The section under which the application is being made'.
- Legal Advisor will liaise with Listings to agree the listing of the application and complete the second part of the pro forma with the details of when, where and how long the application will take. The LA will confirm the arrangement by e-mailing the completed forma to them.
- Administration will email the applicant to confirm date, time and court room of where the application will be heard and the need to bring paper copies of the Information and application; one copy of the Information and three copies of the application. Note at no stage will admin print copies of the Information or Warrant.
- Admin will maintain the generic email box by moving the pending application to a sub file, Monday to Friday for the day of the week when the application will be heard. The subject header of the email will be amended to include the date and time of the application.
- On the date of application the Duty Clerk or available LA will check the generic mail box for any application to be heard on the day. This will become a standing agenda item for team meetings to ensure that applications are not missed.

### **Bulk Applications**

- Applicant to ring the court of application to advise how many applications are required. Thereafter the local authority will be required to submit the application as above.

### **Applications where special circumstances apply**

- Applicant telephones the court of application to advise that application is to be made.
- The administrator will identify the Legal Advisor who will take responsibility for the application(s)

- Local authority to email the information and application to the identified Legal Advisor's personal mail box.

### **Upon arrival at Court**

- The applicant/authorising officer will bring one paper copy of the information and 3 paper copies of the application to Court and pass to the Legal Advisor.
- Upon issue of the application the applicant/authorising officer will be given 3 copies of the application in readiness for execution.

### **After issue**

- Legal advisor will pass the Information to the administration for retention and notation. Documents will be filed in date of application order. The electronic copy of the email should be deleted from the generic email box.
- Following approval the applicant/authorising officer is required to cancel or renew the application within 3 months for directed surveillance and 12 months for CHIS (1 month if under 18) all other instances via internal mail addressed to Admin Team Leader. There is an expectation that the local authority will monitor the returns to the issuing court of the respective application within the prescribed time limits to comply with regulations.
- Upon approval of the application the admin team will update the spreadsheet and file the application with the information.
- In the event of the warrants not being returned to Court within the prescribed timescales, admin will write to the applicant.

### **Out of hours applications**

In relation to urgent applications which cannot be dealt with in office hours, Legal Advisers may be contacted at home. The following numbers are for this purpose only and should not be used for any other enquiries. They must not be disseminated to any other party.

Michael Brassil	0115 939 2466
Sandra Jenkins	01629 733733
Nick Daber	0161 439 9359
Emma Gilberthorpe	(On maternity leave until June 2015)
Lynette Holland	01629 732074
Leonora Salkeld	0114 2364435
Sarah Mettam	01246 471614
Michelle Smith	(On maternity leave until December 2015)
Glyn Plant	07879 002998
Christina Hayes	01629 57408

### **Governance and Access to generic mail boxes**

Access to any Search warrant data or documentation must be treated as highly confidential.

Contact details of the recipient Courts

Court	Generic email address	Telephone
Buxton & Chesterfield	<a href="mailto:DB-Chf-HPSearchWarrants@hmcts.gsi.gov.uk">DB-Chf-HPSearchWarrants@hmcts.gsi.gov.uk</a>	01246 224040
Derby	<a href="mailto:DB-DbySearchWarrants@hmcts.gsi.gov.uk">DB-DbySearchWarrants@hmcts.gsi.gov.uk</a>	01332 333047

The following will have access to the Search Warrant generic email boxes

Buxton and Chesterfield	Derby
All Legal Advisors Emma Mottram Pauline Salt Rachel Spencer Helen Damarell Alistair Cooper	All Legal Advisors Jane Griffiths Dawn Maguire Jane Brearley Sharon Lambert Emma Young Lynda Binch Andrew Goode

- The team Leader responsible for Listing will review the mail box on a monthly basis and report any anomalies to the Operations Manager and Deputy Clerk to the Justices without delay.
- At no stage will the admin be asked to print a copy of the Information or Warrant

Record retention (subject to modification in accordance with HMCTS Records management schedule) – currently:-

RIPA applications	Destroy after 6 years.
-------------------	------------------------

**Bolsover District Council**

**Standards Committee**

**7 January 2016**

**Ethical Standards for Providers of Public Services**

**Report of the Monitoring Officer**

This report is public

**Purpose of the Report**

- To advise Committee of new guidance issued by the Committee on Standards in Public Life (CSPL) on Ethical Standards for the Providers of Public Services.

**1 Report Details**

- 1.1 In 2014, the Committee considered a report on ethical standards for providers of public services. It was acknowledged that many services are now provided by third parties on behalf of councils and it was important for these providers to adhere to the same principles required by local authorities. The report made a number of recommendations to Government to ensure that proportionate ethical standards were being made in commissioning and contracting.
- 1.2 The purpose of this latest report is to provide a short practical guide on building and embedding ethical standards in an organisation and in setting ethical expectations for the delivery of services and ensuring they are met. Included are some examples used by commissioners to build high standards.
- 1.3 It is presented to this Committee for information.

**2 Conclusions and Reasons for Recommendation**

- 2.1 To enable the Committee to consider the report.

**3 Consultation and Equality Impact**

- 3.1 N/A

**4 Alternative Options and Reasons for Rejection**

- 4.1 N/A

## 5 Implications

N/A

## 6 Recommendations

- 6.1 Committee notes the report from the Committee on Standards in Public Life around ethical standards for providers of public services.

## 7 Decision Information

<b>Is the decision a Key Decision?</b> (A Key Decision is one which results in income or expenditure to the Council of £50,000 or more or which has a significant impact on two or more District wards)	No
<b>District Wards Affected</b>	N/A
<b>Links to Corporate Plan priorities or Policy Framework</b>	N/A

## 8 Document Information

<b>Appendix No</b>	<b>Title</b>
A	Ethical Standards for the Providers in Public Services
<b>Background Papers</b> (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)	
<b>Report Author</b>	<b>Contact Number</b>
M Kane	7753

Report Reference –



Committee on  
Standards in  
Public Life

December 2015

# Ethical Standards for Providers of Public Services - guidance

# Contents

---



# Foreword

---



In June 2014 CSPL published a report on Ethical Standards for Providers of Public Services.<sup>1</sup> The government has made clear that the Seven Principles of Public Life first set down by Lord Nolan - honesty, integrity, accountability, leadership, openness, selflessness and objectivity - should apply to all those delivering services to the public. The definition of each of these Principles is set out at the end of this document. Our report considered how these Principles were being built into the public service commissioning and contracting and drew on research conducted for the Committee by Ipsos MORI with commissioners of services, providers of those services and members of the public.

It was clear from our research that the public want all providers of public services to adhere to and operate by common ethical standards, regardless of whether those services are provided by the private, public or voluntary sectors. For the public “how” things are done is as important as “what” is done. The report made a number of recommendations to government to ensure that proportionate ethical standards are made explicit in commissioning, contracting and monitoring and that these standards apply to anyone delivering public services on

behalf of the taxpayer. It also recommended that providers ensure they have a high level ethical framework and ethical capability, encompassing principled leadership and governance, clear lines of accountability and encouraging a culture of dialogue, challenge and transparency. I was delighted by the positive response the report received from commissioners and providers including from the business community.

The purpose of this document is to emphasise the key messages from our report and build on its research and conclusions by providing short practical guidance to both providers of public services in building and embedding ethical standards in an organisation, and to commissioners in setting ethical expectations for the delivery of public services as well as ensuring those standards are met. The Committee recognises the efforts and investments which many providers have already made in enhancing awareness of, and adherence to high ethical standards. The Committee recognises the challenges faced by any organisation large or small in ensuring that all employees adhere to high ethical standards of behaviour. We know that standards failures represent a significant

organisational risk which is why the Committee supports the development and use of appropriate systems and processes to encourage and reinforce ethical behaviour.

We have included some examples of mechanisms used by commissioners and providers to build high ethical standards but are always keen to learn more, so if you know what works please get in touch.

Ethics matter. This is increasingly recognised by the business community as a necessary part of winning trust and building confidence in the public service markets. Ethical standards should not be taken for granted. Commissioners and providers need to be explicit with each other and the public as to the standards expected in the services which are being delivered.

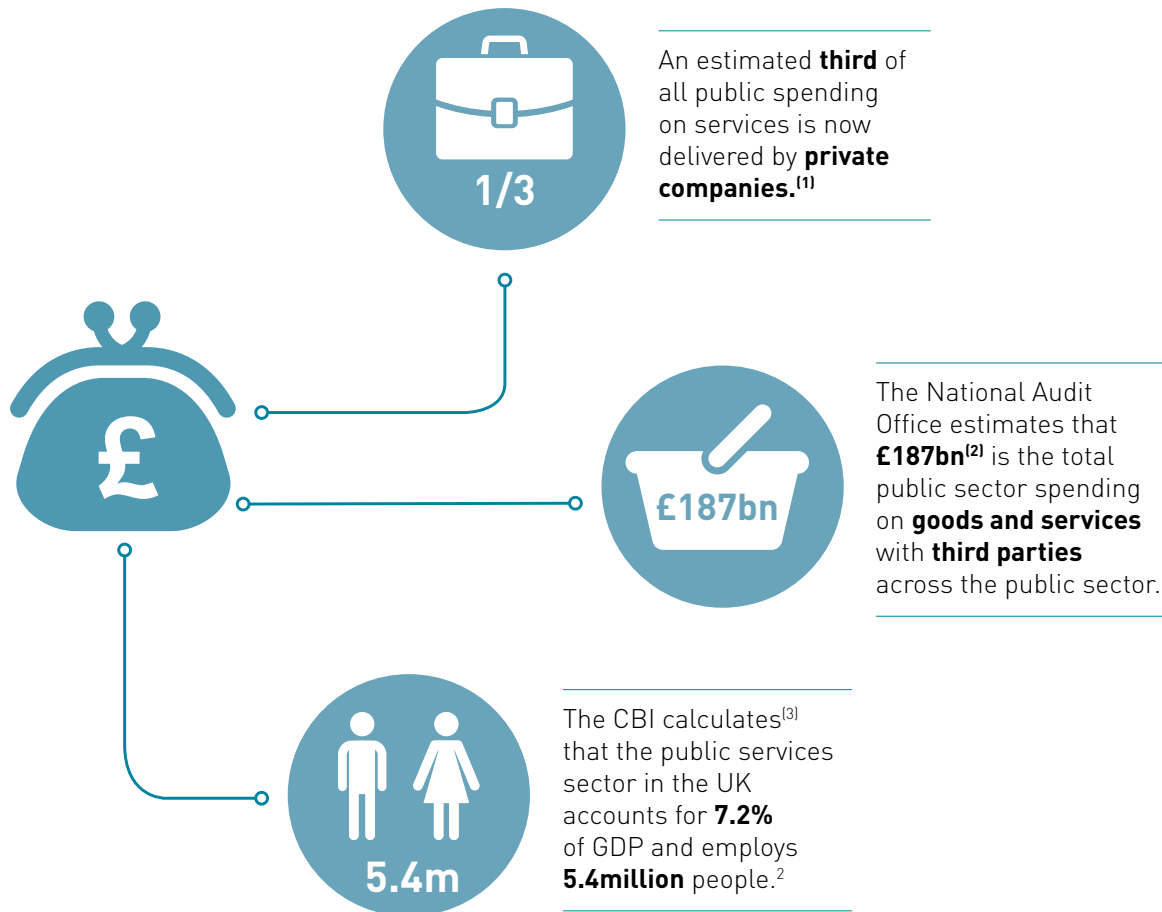
**Lord Bew, Chair of the Committee**

December 2015



# Background to the report

---



It makes good business sense to heighten awareness of ethical standards and encourage their staff to adhere to them. Whilst this may involve a cost, organisations need to invest in this aspect of their business. Ethical failures by banks, the press, and most recently in parts of the car manufacturing industry, carry a heavy price. Ethical failures in the NHS, the police and in the public service market more generally have all demonstrated that the damage to reputation and trust, and the financial cost to the business or provider concerned, can be high. Ethical failure by a significant provider of public services can be a major risk to the Government, and can have broader implications for the level of public trust and confidence in the Government and its ability to deliver public services.

# About our report

---

In our report, Ethical Standards for Providers of Public Services, we proposed a high level framework to support and embed high ethical standards in the provision of public services and to provide the necessary assurance to the public and the government that ethical standards are part of service delivery standards. This framework was based around principled leadership and governance including a code of conduct, a culture of dialogue and challenge, clarity of accountability and ethical capability and transparency.

---

## The CBI:

**“200 000 charities and companies of all sizes help government provide the public services that we depend on all over the country. This can generate innovation, investment and efficiency, but also requires standards of conduct that are appropriate for organisations funded by and working for taxpayers.”**

---

For the full report: [www.gov.uk/government/publications/ethical-standards-for-providers-of-public-services](http://www.gov.uk/government/publications/ethical-standards-for-providers-of-public-services)

High ethical standards are important for society as a whole. They are particularly important where public money is being spent on public services or public functions as commissioning and procurement decisions can have a major impact on the user's daily lives and their quality of life. When a provider fails to deliver to the standards expected, and particularly where the user may have no other choice, it may have profound consequences for the individual user and damage public trust more generally.

High ethical standards are important for society as a whole. They are particularly important where public money is being spent on public services or public functions. Commissioning and procurement decisions can have a major impact on the users daily lives and their quality of life. When a provider fails to deliver to the standards expected, particularly where the user may have no other choice, it may have profound consequences for the individual user and damage public trust more generally.

## Public Accounts Committee:

**“Contractors have not shown an appropriate duty of care in the use of public funds. Too often the ethical standards of contractors have been found wanting. It seems that some suppliers have lost sight of the fact that they are delivering public services, and that brings with it an expectation to do so in accordance with public service standards. The legitimate pursuit of profit does not justify the illegitimate failure to conduct business in an ethical manner.”<sup>3</sup>**

---

**Mark Galloway, Executive Vice President, Skanska UK:**

**“It has to be recognised that our approach to ethics and embedding ethical behaviours in our business is a journey. We are not the finished article, so we always have more to do.**

**The benefits, however, are significant. It helps us to attract employees who want to work for an ethically driven business, build long and lasting relationships with our supply chain partners and, ultimately, to win work. Being a leader in ethics makes good business sense.**

**It is by putting the right framework in place, setting the highest standards and encouraging our employees to become role models for ethics that we can establish a best in class ethical culture.”**

---

It is therefore incumbent on those bodies commissioning and procuring public services, and those who are ultimately responsible and accountable for those services, to obtain assurance that high ethical standards are being met. Accountability does not end and should not dissipate on the commissioning or contracting out of public services.

Whilst many of the requirements for high standards require action at an organisational level, high standards also require individuals to take personal responsibility - by observing high standards themselves, by demonstrating high standards to others through their own behaviour and by challenging inadequate standards when they see them.

In an earlier report, Standards Matter, (14<sup>th</sup> Report January 2013 Cm 8519), the Committee stated that high standards of behaviour need to be seen as a matter of personal responsibility, embedded in organisational processes and actively and consistently demonstrated, especially by those in leadership positions. One of that report's conclusions was that permanent secretaries and chief executives of all organisations delivering public services should take personal responsibility for ethical standards in their organisations and certify in their annual report or equivalent document that they have satisfied themselves about the adequacy of their organisation's arrangements for safeguarding high standards.

The need for leaders and managers within an organisation to model high ethical standards and to take personal responsibility for their behaviour means that high ethical standards may take time to become established within an organisation. Ethical standards cannot be “fixed” onto an organisation overnight and then forgotten. It takes time for an ethical culture to become the norm and requires regular communications to staff to reaffirm ethical practice and behaviours.

### **Key conclusions from the report**

The research conducted for the Ethical Standards for Providers of Public Services report found that:

- the public want the same ethical standards upheld by any organisation providing public services regardless of sector and supported by a code of conduct
- public and stakeholder views of what should constitute ethical standards are broadly in line with the Seven Principles of Public Life
- “how” the service is delivered is as important to the public as “what” is delivered
- the public felt good outcomes and quality of user/provider interaction - particularly from front line staff behaving with integrity and objectivity - were crucial to ethical service delivery

## Quotes from the public

“If it’s taxpayers’ money, the principles are the guidance and all providers should follow them.”

“(They should have) end users’ best interests in mind”

- commissioners expect providers to conform to ethical standards but rarely explicitly articulate ethical standards to providers explicitly;
- commissioners want guidance on how to embed ethical standards in the commissioning and procurement process.

It was also evident from the research that currently there are no consistent structures or arrangements within the commissioning process to promote actively the right ethical culture and behaviours in providers of public services.

The report therefore recommended that ethical standards need to be proportionately addressed within existing commissioning, contractual and monitoring arrangements, as part of the process for securing the regularity and propriety of public services.

## Quotes from Commissioners and Providers

“It is up to commissioners to be clear about what they want and expect from suppliers, otherwise the contract is won on price”

“As things stand now, contractors see that they are not being watched and become complacent.”

There has been much debate about increasing transparency in public service contracts. Whilst we agree that one route to improving public service standards is through greater transparency and, particularly in the case of larger service providers, the application of the Freedom of Information Act, transparency of itself is not sufficient. Transparency needs to be underpinned by a culture of high ethical standards in public service contracts.

# Follow on work

---

Following our report we undertook further work, including workshops and discussions with commissioners and providers, to review how they are adapting their procedures and practices to ensure the highest possible ethical standards are adopted and adhered to by staff in their organisations delivering public services.

In addition, we have also identified more extensive examples of good practice in a range of commissioners and providers which might be applied more widely. These organisations recognise the challenge of encouraging their employees to behave with high ethical standards at all times and have adopted a variety of systems and processes to support their employees. And they recognise that an

ethical culture is not achieved by a one-off effort, but through the continuing attention to the importance of ethical behaviour.

This guidance document is intended to provide practical guidance and examples to commissioners and providers in setting and embedding those standards of conduct and agreeing the ethical expectations for the delivery public services. Any ethical framework should be risk-based, flexible and proportionate. How it is implemented in practice will depend on the nature of the public service being provided, the model of delivery and the kind of provider.

The National Audit Office has recommended that government should get “*written representation from contractors on the integrity of the services they supply, covering the control environment for maintaining ethical behaviour and public service standards. Such statements, while not necessarily carrying additional legal implications, would have symbolic and reputational importance, and give Parliament clear accountability.*”<sup>4</sup>

**Ruby McGregor Smith**  
**Chair of the Public Services**  
**Network CBI:**

“Every organisation has a process around governance, around the controls it exhibits and around its behaviours. It can be done, it just needs to be done and clearly laid out in contracts we are asked to sign, so that everyone does it.”<sup>5</sup>”

**Melanie Maxwell Scott**  
**Business Services Association:**

“High ethical standards can and should be achieved by any public service provider. The sector they come from is not material as long as expectations are made clear and there exists a culture which supports good behaviour and promotes prompt action whenever people fall short.

Procurement and contract-management processes are vital to aligning the values of the public sector client with any supplier. If a contract is poorly written, the wrong type of behaviour can occur or even be encouraged. If the contract is poorly managed, sub-standard performance can go unnoticed. That is in no-one’s best interests, least of all the service user.”<sup>6</sup>”

# Suggested Measures

Set out below are examples of measures which could be expected of, implemented and embedded by providers of public services and monitored and evaluated by commissioners to provide assurance of ethical standards - how does the organisation do its

business and how do individuals within it carry out their roles?

It is not intended as a burdensome checklist to be ticked and regarded as complete; rather it should

be used to encourage not only commissioners to be explicit about their expectations on ethical standards, but also providers to reflect on their capacity and capability to meet those standards.

<p><b>Evidence of leadership commitment to ethical standards</b> - What is the tone from the top and how is this lived out throughout the organisation? What are the values and behaviours this organisation is encouraging and discouraging?</p>	<p>Public statements and day-to-day behaviour that demonstrate visible commitment to ethical standards and taking responsibility – being publicly accountable – for ethical standards.</p> <p>In a small organisation this could be as simple as telling all staff about the ethical expectations of those in the organisation delivering public services.</p>
<p><b>Evidence of board and individual responsibility for ethical standards</b> - how are employees and (if applicable) board members held to account collectively and individually for ethical issues?</p>	<p>Board level oversight of ethical matters and board level responsibility for or championing of ethical compliance.</p> <p>Ethics committees can be used as a mechanism to improve and scrutinise ethical decision making but they should be integrated to the governance arrangements and not a “bolt-on”.</p> <p>Annual attestations - individual annual sign off of compliance with the company’s Code of Conduct and compliance regulations or policies.</p> <p>Employees are aware of the code of conduct and the consequences of failing to adhere to the Code.</p>

<p><b>Evidence of internal control and accountability measures</b> - what is the internal control environment for maintaining ethical behaviour and standards in the organisation?</p>	<p>A suitable code of conduct - typically a series of Do's and Don'ts, publically available and adherence to the code monitored.</p> <p>Identification of key indicators or measures of an ethical culture within the organisation and periodic reviews of their effectiveness.</p> <p>Existence of and adherence to whistleblowing policy or speak up mechanisms, gifts and hospitality registers, anti-bribery and corruption, declarations of interests requirements, procedures for dealing with conflicts of interest, which are regularly reviewed.</p> <p>Ethical risks captured and controlled in the risk management process and evidence they have been identified, assessed and where required mitigated.</p> <p>Transparency and reporting arrangements which encourages "intelligent accountability" putting out good quality information in intelligible and adaptable formats creating a genuine dialogue with stakeholders.</p>
<p><b>Evidence of establishing an ethical awareness and capability in recruitment, induction, progression, training and professional development</b> - how is ethical awareness embedded in the organisation?</p>	<p>Recruitment procedures that take account of values and ethics alongside other skills.</p> <p>Induction processes that give new starters an understanding of the ethical expectations of them, the Codes of Conduct and ethical framework operating in the organisation.</p> <p>Training and guidance on ethical standards generally through ethical and values based training online and face to face.</p> <p>Self-assessment often web based tools.</p> <p>Employees encouraged to demonstrate achievement of e.g. ethical component of commercial capability requirements such as Chartered Institute of Purchasing and Supply's ethical procurement and supply e-learning module.<sup>7</sup></p>



<p><b>Evidence of appraisal, promotion and reward procedures that take account of values and ethical behaviour</b> - how does the organisation encourage (or not) its intended values and behaviours?</p>	<p>Codes of conduct linked to performance incentives.</p> <p>Assessing staff on behaviour based criteria the “how” as well “what” they have achieved. Assessing behaviours against core values - e.g. do they role model behaviours consistently, do they coach and encourage others to achieve similar high standards, for leaders do they develop a working culture which emphasises integrity and ethics? do they champion the company values?</p> <p>Including questions on ethical matters in employees surveys.</p>
<p><b>Evidence of commissioner-provider and user-provider dialogue</b> - what is the success or failure for this contract including the supply chain and what are the essential behaviours to deliver success? how does the organisation learn from criticism and compliments?</p>	<p>Use of staff feedback surveys and self-assessment.</p> <p>Responding to and acting on feedback.</p> <p>Robust complaints system and evidence of good complaints handling; the effective use of complaints data to evaluate how well standards are being achieved and to help deliver service improvements.</p> <p>Setting out clear expectations and standards throughout the supply chain, monitoring compliance with them and clear explanation provided as to the consequences of failing to meet the standards expected.</p>

# Practical examples and case studies

---

We set out below some further practical examples and case studies of measures or ethical frameworks some organisations have put in place in an attempt to build awareness of and adherence to high ethical standards. These examples were shared with us by the relevant organisations, are illustrative and correct at the time of publication of our reports. We expect that as experience of these arrangements grows they will be further developed.

## Case study - Mitie example of tone from the top

As part of their wider ethical business framework Mitie launched a [new] Code of Conduct in 2014. The Code was designed to help employees understand the core values and responsible behaviours enabling them to “do the right thing”. In addition to setting our core company policies and procedures, the Code aims to bring to life through scenarios some of the ethical dilemmas faced by those working in Mitie and to provide a set of guiding principles to follow.

The Code, core values and responsible behaviour have been visibly championed by the Chief Executive and the Group Finance Director. The Code’s importance was reinforced through a series of initiatives such as:

- The launch of the Code at an Executive Board workshop
- Risk management leadership workshops
- Monthly roadshows across the business attended by the CEO and CFO
- the promotion of the confidential Speak Up service

- The use of all staff emails from the CEO emphasising the importance of core values and responsible behaviours and what it means for the company
- Open lines of communication between CEO and employees such as twitter

### **The NCVO and Good Governance Code for the voluntary and community sector**

This code sets out the principles and practices that should be adopted in those sectors for good governance. It can be applied in a flexible way depending on the type and size of the organisation. It covers behavioural governance including the effective board behaving with integrity and being open and accountable. It recognises the applicability of the seven principles of public life to the sector as recognised good practice and complementary to those principles.

[www.governancecode.org](http://www.governancecode.org)

---

## Case study – Skanska’s ethical business practices

---

Skanska, one of the UK’s leading contractors, is an inclusive and responsible business that is helping to build a better society. Known for major projects, such as the Gherkin and Crossrail, it is building, upgrading and maintaining the country’s infrastructure – delivering projects in healthcare, education, defence, transportation and municipal services. Drawing on its Scandinavian heritage, it is green, innovative and progressive. Bringing together people and technology, it is working to make construction a safer and more collaborative industry.

Ethics is a core value for Skanska, which is placed at the heart of its business. It has an aim to be recognised for its commitment to doing the right thing, everywhere that it works.

To make this a reality, it has a range of tools that help to bring ethics to life, demonstrating what it means for its employees.

### Ethics Roadmap

Launched as a global tool, the Ethics Roadmap is designed as a practical document that helps

Skanska’s national operations to develop an internal culture and behaviour in the market that is best in class.

### Ethics Scorecard

Used to monitor the progress of ethics in national Business Units and throughout Skanska. The Ethics Scorecard is published twice a year with the latest data and examples of best practice to share across the organisation.

### Ethics champions

Each global business unit has appointed a senior-level Ethics Champion responsible for driving ethical behaviour and implementation of the Ethics Roadmap. This includes development of an annual ethics plan, which sets out the actions which will be taken over the coming year to help build an ethical culture.

### Code of Conduct

Skanska’s Code of Conduct applies to all employees and the principles bind Skanska’s supply chain too. All employees participate in Code of Conduct training every two years, and new recruits within three months of joining. <http://www.skanska.co.uk/About-Skanska/Our-Code-of-Conduct/>

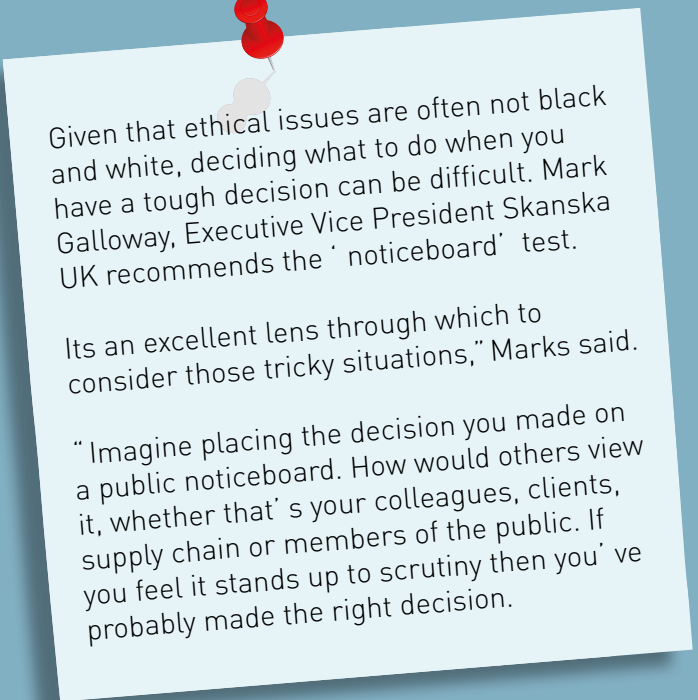
### Ethical dilemmas

at least four times a year, all employees take part in informal ethical debates. There are no right or wrong answers, the aim is to facilitate discussion

and encourage employees to feel comfortable discussing ethical dilemmas in business. The ‘notice-board test’ is often referenced – if your decision was posted on a public notice-board, would you stand by your actions?

### Annual employee survey

All employees are asked two ethics-related questions as part of the annual employee survey, so understanding and attitudes can be effectively monitored.



Given that ethical issues are often not black and white, deciding what to do when you have a tough decision can be difficult. Mark Galloway, Executive Vice President Skanska UK recommends the ‘noticeboard’ test.

Its an excellent lens through which to consider those tricky situations,” Marks said.

“Imagine placing the decision you made on a public noticeboard. How would others view it, whether that’s your colleagues, clients, supply chain or members of the public. If you feel it stands up to scrutiny then you’ve probably made the right decision.

### **Code of Conduct Hotline**

An independent Code of Conduct hotline has been set up, which enables employees to report concerns about ethical behaviour, anonymously if they wish.

### **Governance**

Two groups have been created to govern ethics in Skanska's UK business. The Ethics Committee, which drives policy development and provides advice, and the Ethics Representatives, which helps to communicate ethics ideas and messages across the business.

### **Defra's Ethical Procurement Policy Statement**

This statement sets out that Defra's expectation that its suppliers will maintain high standards of integrity, professionalism and transparency and how working in partnership with suppliers it will address wider ethical issues outside the public procurement process. These issues include working conditions, employee health and training, discrimination and child labour.<sup>8</sup> The policy aims to achieve wider societal benefits

through ethical principles such as requiring "suppliers [to] have systems in place to ensure high standards of propriety which make sure public money is used for the purpose it is intended." Defra was able to point more easily than some Departments, to mechanisms which existed throughout the commissioning and procurement process including pre and post award stages.

## Case study – Embedding the College of Policing’s Code of Ethics

The College of Policing’s Code of Ethics is applicable to all members of the police force and places an additional responsibility on chief officers and leaders to promote and reinforce the Code amongst the wider police force. In its recent report on local police accountability - *Tone from the top - leadership, ethics and accountability in policing?*, the Police Superintendents Association of England and Wales, shared with the Committee evidence from the Thames Valley police force about their experience embedding the Code of Ethics. The research found that the most effective code was part of a broader programme of culture change and should be regularly reinforced and monitored.

Thames Valley Police Force research - Code of Ethics	
What works	What hurts
Value-based approach to ethics programmes	
Ethical culture, supported by ethical programme	Standalone ethical programme
Ethical discussion and rewarding ethical behaviour	Too much focus on punishing lack of compliance to the code Unquestioning obedience
Focus on colleagues or society	Focus on self-interest
More time for decision-making promotes ethical behaviour	Rushed decision-making encourages unethical behaviour
Challenging unethical practice	Ignoring unethical practice
Peer influence (positive)	Peer influence (negative)
Thoughtful implementation of goals and targets	Carelessly implemented goals and targets
Regularly reinforcing ethical behaviours Immersive ethical training	

More important for people to know that the organisation is fully committed to code, rather than knowing all the content of the Code of Ethics	
Moral reasoning by leaders	
Fairness and respect	

---

## PwC ethical decision making

---

**Tina Hallett**  
**PwC Partner, Government and**  
**Public Sector Leader:**

High ethical standards can and should be achieved by any public service provider. The sector they come from is not material as long as expectations are made clear and there exists a culture which supports good behaviour and promotes prompt action whenever people fall short.

PwC the professional services network reinforces the messages of induction by making it clear that ethics is integral to the operation of the firm. PwC has a dedicated Ethics and Business Conduct section on its website, which includes a code and a framework for ethical decision making, as well as a list of ethics questions to consider when making day-to-day decisions.<sup>10</sup> There is a clear narrative that ethical standards are integral and important, which in turn make the messages of induction that much more likely to be absorbed and taken seriously.

### Summary of ethics questions to consider

1. Is it against PwC or professional standards?
2. Does it feel right?
3. Is it legal?
4. Will it reflect negatively on you or PwC?
5. Who else could be affected by this (others in PwC, clients, you, etc.)?
6. Would you be embarrassed if others knew you took this course of action?
7. Is there an alternative action that does not pose an ethical conflict?
8. How would it look in the newspapers?
9. What would a reasonable person think?
10. Can you sleep at night?

---

## Case study – Network Rail

---

**‘ Our reputation and future depends on us all  
behaving with integrity in everything we do’**

**Mark Carne, CEO**

On the 1st September 2014 Network Rail was reclassified as a public sector body. While passengers won't have noticed a difference to the running of the railway, the impact on some areas of our work has been more pronounced.

One consequence of our new status is that we are now subject to the principles of public life. These are an important reminder to everyone who works for or does business with Network Rail of the importance of acting with the highest possible levels of integrity. We welcome the scrutiny and accountability that comes with being part of the public sector, and strongly believe that an open, ethical and fair culture is fundamental to how we operate, every day.

But our work to drive the highest levels of business behaviour is not a knee jerk response to reclassification. We have had a Code of Business Ethics for a long time, and it is complemented by a busy business ethics programme. Our priority this year is delivering ethics training to all our staff – our training packages all have the principles of public life running through them. The Code is supported by a number of policies including anti bribery, gifts & hospitality, conflict of interests, social media and speak out (whistleblowing). We have also set up a register for gifts, hospitality and conflicts of interests called iEthics, and a confidential whistleblowing service, Speak Out.

We launched Speak Out in its current form in 2012 to help our employees and contractors report ethical misconduct. They can do so over the phone or through a secure website. Use of the service has increased steadily over its lifetime, and we have also seen a gradual decrease in the proportion of users who choose to report anonymously. We think this shows that people are beginning to feel more comfortable speaking out about suspected wrongdoing, which is an important indicator of our progress towards the culture we want across the company.

We still have work to do to change the culture of our organisation, but we think we are on the right path. Network Rail has a responsibility to the nation to run a safe, reliable railway, and ethical values like openness, integrity and accountability are at the core of our ability to do so.

---

## Case study – Dudley Metropolitan Borough Council “Supplier Code of Practice”

---

“Supplier Code of Practice” sets out the values, principles and standards Dudley Council expects of itself and its suppliers. It covers the Seven Principles of Public Life and their application to employees and suppliers, and specific expectations in relation to bribery and corruption, gifts and hospitality, conflicts of interest, fraud, deception and dishonesty, false claims, unfair trading and competition and environmental issues. It also provides details of how to raise any concerns that the code is not being complied with.

<http://www.dudley.gov.uk/business/do-business-with-the-council/tenders-and-contracts/trade-with-dudley/>

### Councillor Pete Lowe:

“As Leader of Dudley Metropolitan Borough Council I want everyone to help us work in partnership to deliver high quality services which recognise our commitment to the highest standards of ethics and conduct. Our Council Plan reflects on this by including a key message of everyone articulating and living up to a set of values and behaviours that support good governance.

The public expect the highest standards of ethics from all suppliers of public services and our message to staff and suppliers is clearly articulated in our “Supplier Code of Practice”. We will be asking major suppliers to confirm that they adhere to the Code in all their dealings with the Council and residents of Dudley. We have a Code of Conduct for employees and councillors which also set out our requirement for them to demonstrate the highest standards of conduct”





---

## Case study – Sodexo Public Sector Pledge

---

In the UK and Ireland, Sodexo employs around 34,000 people across 1,850 locations in the corporate, healthcare, education, leisure, justice and defence sectors. Sodexo delivers a range of services, from catering and hospitality, cleaning, reception to asset management, security, laboratory and grounds maintenance services.

As a company with half its business in the public sector, in 2015 Sodexo published its Public Sector Pledge. The aim of the Pledge is to be an 'ethical manifesto' identifying key public service areas and initiatives which Sodexo will publicly measure and report on annually. Areas covered by the Pledge include client satisfaction reviews, outcome based contracts, business integrity codes and adoption of the living wage.

### The pledge focuses on three key themes:

1. fully committed to consistent delivery of our promises, your outcomes, and your value for money;
2. Transparent and truly ethical in how we deliver in our use of public money, and in our conduct;
3. Enhancing quality of life and social justice in our communities through a genuine social conscience.

Through this pledge Sodexo states it hopes to achieve better public services, end stereotypes, to grow and succeed as a business and to do the right thing.

In June 2015, Sodexo joined the Living Wage Foundation's Recognised Service Provider scheme, committing to implement the UK and London Living Wage for all employees working in its head offices in London, Glasgow, Stevenage, Leeds, Salford and Swindon. the commitment also means that Sodexo will, wherever permitted, submit a Living Wage alternative in all its bids and will promote the adoption of the living wage to its clients.

Sodexo intends to publish the progress it has made with each of the commitments within the Pledge around the middle of 2016.

<http://uk.sodexo.com/uk/en/corporate-responsibility/responsible-employer/public-service-pledge.aspx>

**Merlin Standard** is designed to recognise and promote sustainable excellence within supply chains. Its aim is to encourage excellent supply chain management and to ensure fair treatments of partners and subcontractors by the Prime Contractor. The principles on which it is built include Conduct and elements of the assessment of the organisation validated by supply chain partners includes such criteria as "culture in which communication is open, honest and without unreasonable constraint", "procurement processes are fair and transparent", it "actively seeks users feedback...to inform and improve practices."

[www.merlinstandard.co.uk](http://www.merlinstandard.co.uk)



# About the Committee on Standards in Public Life

---

1. The Committee on Standards in Public Life is an advisory Non-Departmental Public Body (NDPB) sponsored by the Cabinet Office. The Chair and members are appointed by the Prime Minister. The Committee was established in October 1994, by the then Prime Minister, with the following terms of reference:

*“To examine current concerns about standards of conduct of all holders of public office, including arrangements relating to financial and commercial activities, and make recommendations as to any changes in present arrangements which might be required to ensure the highest standards of propriety in public life.”*

2. The remit of the Committee excludes investigation of individual allegations of misconduct.
3. On 12 November 1997 the terms of reference were extended by the then Prime Minister:

*“To review issues in relation to the funding of political parties, and to make recommendations as to any changes in present arrangements.”*

4. A triennial review of the Committee was carried out in 2012, the report of which was published by the Government in February 2013. As a result, on 5 February 2013, the terms of reference of the Committee were clarified in two respects: ‘... in future the Committee should not inquire into matters relating to the devolved legislatures and governments except with the agreement of those bodies’ and ‘...the Committee’s remit to examine “standards of conduct of all holders of public office” [encompasses] all those involved in the delivery of public services, not solely those appointed or elected to public office.’

## Membership of the Committee

The Lord Bew (Chair)  
The Lord Alderdice  
The Rt Hon Dame Margaret Beckett DBE MP

Sheila Drew Smith OBE  
Patricia Moberly  
Richard Thomas CBE  
Dame Angela Watkinson DBE MP  
Monisha Shah

## The Committee’s previous reports

5. The Committee has previously published the following reports.
  - Tone from the Top - leadership, ethics and accountability in policing, June 2015
  - Ethical standards for providers of public services, June 2014
  - Strengthening Transparency Around Lobbying, November 2013
  - Standards Matter: A review of best practice in promoting good behaviour in public life (Fourteenth Report), Cm 8519, January 2013

- Political party finance: Ending the big donor culture (Thirteenth Report), Cm 8208, November 2011
  - MPs' expenses and allowances: Supporting Parliament, safeguarding the taxpayer (Twelfth Report), Cm 7724, November 2009
  - Review of the Electoral Commission (Eleventh Report), Cm 7006, January 2007
  - Getting the balance right: Implementing standards of conduct in public life (Tenth Report), Cm 6407, January 2005
  - Defining the boundaries within the Executive: Ministers, special advisers and the permanent civil service (Ninth Report), Cm 5775, April 2003
  - Standards of conduct in the House of Commons (Eighth Report), Cm 5663, November 2002
  - Standards of conduct in the House of Lords (Seventh Report), Cm 4903, November 2000
  - Reinforcing standards: Review of the First Report of the Committee on Standards in Public Life (Sixth Report), Cm 4557, January 2000
  - The funding of political parties in the United Kingdom (Fifth Report), Cm 4057, October 1998)
  - Review of standards of conduct in executive NDPBs, NHS trusts and local public spending bodies (Fourth Report), November 1997
  - Local government in England, Scotland and Wales (Third Report), Cm 3702, July 1997
  - Local public spending bodies (Second Report), Cm 3207, June 1996
  - Members of Parliament, ministers, civil servants and quangos (First Report), Cm 2850, May 1995
6. The Committee is a standing Committee. It can not only conduct inquiries into areas of concern about standards in public life, but can also revisit those areas and monitor whether and how well its recommendations have been put into effect.

# Seven principles of public life

---

The Seven Principles of Public Life<sup>11</sup> apply to anyone who works as a public office-holder. This includes all those who are elected or appointed to public office, nationally and locally, and all people appointed to work in the civil service, local government, the police, courts and probation services, NDPBs, and in the health, education, social and care services. All public office-holders are both servants of the public and stewards of public resources. The Principles also have application to all those in other sectors delivering public services.

## **Selflessness**

Holders of public office should act solely in terms of the public interest.

## **Integrity**

Holders of public office must avoid placing themselves under any obligation to people or organisations that might try inappropriately to influence them in their work. They should not act or take decisions in order to gain financial or other material benefits for themselves, their family, or their friends. They must declare and resolve any interests and relationships.

## **Objectivity**

Holders of public office must act and take decisions impartially, fairly and on merit, using the best evidence and without discrimination or bias.

## **Accountability**

Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.

## **Openness**

Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.

## **Honesty**

Holders of public office should be truthful.

## **Leadership**

Holders of public office should exhibit these principles in their own behaviour. They should actively promote and robustly support the principles and be willing to challenge poor behaviour wherever it occurs.

## **Committee on Standards in Public Life**

GC05 1 Horse Guards Road, London, SW1A 2HQ  
<https://www.gov.uk/government/organisations/the-committee-on-standards-in-public-life>

# References

---

- <sup>1</sup> <https://www.gov.uk/government/publications/ethical-standards-for-providers-of-public-services>
- <sup>2</sup> [1] Julius, D., *Public Services Industry Review*, 2008, Retrieved 15 July 2013: <http://www.bis.gov.uk/files/file46965.pdf>. Note that this estimate includes services procured by government to support service delivery cited in Institute for Government 2012 Testing New Commissioning Models A guide to help policy makers learn about publically funded markets.
- [2] *The role of major contractors in the delivery of public services*. National Audit Office HC 810 Session 2013-14 12 November 2013.
- [3] CBI, *A Value Driven Public Services Sector* page 6 Oxford Economics analysis for CBI.
- <sup>3</sup> Committee of Public Accounts Transforming contract management Twenty-third report of Session 2014-15 HC 585 10 December 2014
- <sup>4</sup> National Audit Office Report, Cabinet Office, Transforming government' s contract management, para 3.17. HC 269 Session 2013-14, 4 September 2014.
- <sup>5</sup> Oral evidence: Contract management within central Government Wednesday 10 September 2014 HC 586 p, 6.
- <sup>6</sup> CSPL Blog 26 March 2015 <https://cspl.blog.gov.uk/2015/03/26/commissioners-and-businesses-can-achieve-high-ethical-standards-by-working-together/>
- <sup>7</sup> <https://www.cips.org/en-GB/training-courses/Ethical-Procurement-and-Supply-/>
- <sup>8</sup> Ethical Procurement Policy Statement March 2011. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/69421/ethical-procurement-policy-statement.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/69421/ethical-procurement-policy-statement.pdf)
- <sup>9</sup> <https://www.gov.uk/government/publications/tone-from-the-top-leadership-ethics-and-accountability-in-policing>
- <sup>10</sup> See <http://www.pwc.com/gx/en/ethics-business-conduct/code-of-conduct.jhtml>, and <http://www.pwc.com/gx/en/ethics-business-conduct/ethics-questions.jhtml>
- <sup>11</sup> The Seven Principles were established in the Committee' s First Report in 1995; the accompanying descriptors were revised following a review in the Fourteenth Report, published in January 2013.



Complaints of Breach of the Code of Conduct – 2015

Year	Number Received	PC	DC	Monitoring Officer's decision in consultation with the Independent Persons – action other than investigation.	Investigation	Hearing	Outstanding.
<b>MC JAN 1/2015</b>	1	√		<b>NFA</b>			
<b>MC MAY(1) 2/2015</b>	2		√	<b>NFA</b>			
<b>MC MAY (2) 3/2015</b>	3	√		<b>NFA</b>			
<b>MC JULY 4/2015</b>	4	√		<b>NFA</b>			
<b>MC SEPT (1) 5/2015</b>	5	√		<b>NFA</b>			
<b>MC SEPT(2) 6/2015</b>	6	√		<b>NFA</b>			
<b>MC SEPT(3) 7/2015</b>	7	√		<b>NFA</b>			
<b>MC SEPT (4) 8/2015</b>	8	√		<b>NFA</b>			
<b>MC SEPT (5) 9/2015</b>	9	√		<b>NFA</b>			
<b>MC NOV (1)</b>	10	√		Ongoing			

<b>10/2015</b>							
<b>MC NOV (2) 11/2015</b>	11	√		Ongoing			

Number (in addition to the above) rejected as being out of jurisdiction





**STANDARDS COMMITTEE WORK PLAN 2015/16**

ITEM	MILESTONES	DATES OF MEETINGS	COMMENTS	STATUS
1. Annual report to Council by Chairman of Standards Committee		<ul style="list-style-type: none"> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• Suggested date - July or August 2016 Council</li> </ul>	
2. Review of training needs – District and Parish Councillors	<ul style="list-style-type: none"> <li>• District Councillors</li> <li>• Parish Councillors</li> <li>• Monitoring of attendance</li> </ul>	<ul style="list-style-type: none"> <li>• Progress reports at each meeting</li> </ul>	<ul style="list-style-type: none"> <li>• District Cllrs – Through Member Development Working Group.</li> <li>• Parish Cllrs –</li> </ul>	
3. Annual Reports -	<ul style="list-style-type: none"> <li>• Year end number of complaints against District and Parish Councillors.</li> <li>• Gifts and hospitality Registers</li> <li>• RIPA</li> </ul>	<ul style="list-style-type: none"> <li>• Progress reports at each meeting.</li> <li>• .</li> <li>• .</li> </ul>	<ul style="list-style-type: none"> <li>• The figures, including the previous years figures, are reported at each meeting</li> <li>• April 2016</li> <li>• April 2016.</li> </ul>	<ul style="list-style-type: none"> <li>•</li> </ul>
4. Review of standards framework	<ul style="list-style-type: none"> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• Annual review</li> </ul>	<ul style="list-style-type: none"> <li>•</li> </ul>

ITEM	MILESTONES	DATES OF MEETINGS	COMMENTS	STATUS
5. Review of RIPA Policy	•	• .	• Annual review. The revised draft Policy is to go to the Joint Strategic Alliance Committee on the 8 <sup>th</sup> December. The revised policy is an item on this agenda.	•
6. Review of whistle blowing policy	•	• .	• Annual review	•
7. Review of Constitution	• Through Constitution Working Group		• Light touch review	•
8. Update on consideration of Rotherham report.	•		•	•
9. Development of the Annual Standards Committee work plan for 2016 to 2017	•	•	•	

June 2015