



Executive Authority Policy (Surrey and Sussex) (1220/2024)

Abstract

This policy covers 'directed surveillance' outside of the Regulation of Investigatory Powers Act 2000 (RIPA).

Policy

1. Introduction

1.1 Intention

The use of this policy will govern the respective Force Professional Standards Department (PSD) and Anti-Corruption Unit (ACU) when conducting 'directed surveillance' outside of the [Regulation of Investigatory Powers Act 2000](#) (RIPA). Directed Surveillance is defined as per [Part 2 of RIPA](#).

2. Scope

2.1 This policy sets out the rationale for lawful and ethical surveillance of police officers or police staff (to include Surrey Police and Sussex Police officers, police staff, Special Constables / volunteers and contractors, (hereafter referred to as officers and staff)) to investigate allegations that may amount to misconduct but where no criminal proceedings are likely to be sought and / or no criminal offences are suspected of having been committed or cases which are criminal but not investigated as such.

3. Policy Statement

3.1 All Surrey Police and Sussex Police (hereafter referred to as the Forces) officers and staff are obligated to adhere to the principles of professional behaviour documented in the Code of Ethics and to ensure that no action damages public trust and confidence. Allegations of corruption or misconduct / breaches of the Code of Ethics or Standards of Professional Behaviour will usually be investigated overtly but there will be occasions, where instead a covert investigation is undertaken.

Procedure

1. Anti-Corruption Unit (ACU)

1.1 Surrey Police and Sussex Police each have their own ACUs who work within Professional Standards Department (PSD) – all UK police and law enforcement agencies have a similar unit which is sometimes referred to as the Counter Corruption Unit (CCU) or PSD Intelligence Unit. The ACUs conduct covert investigations in support of misconduct and criminal matters involving Surrey Police and Sussex Police officers,

police staff, Special Constables / volunteers / contractors or external persons seeking to corrupt the same.

1.2 Where the alleged behaviour is an allegation that, if proved, might constitute a criminal offence by any of these persons then the principles of any criminal investigation will be adhered to, and any surveillance will be sought in line with Regulation of Investigatory Powers Act 2000 (RIPA) following the guidance and authorisation process of the respective Force. In such instances Executive Authority will not be used.

1.3 The extent of surveillance that can be authorised under an Executive Authority is defined as 'directed surveillance' under Part 2 of RIPA. 'Intrusive surveillance' as defined under the same Act cannot be authorised under Executive Authority. In addition to 'directed surveillance' Executive Authority may also specifically be used to covertly monitor telephone calls made through the Forces telephony systems or other corporate devices or to utilise ambient listening of issued devices. Interference with police owned or controlled property may also be authorised to facilitate an Executive Authority authorisation.

2. About this procedure

2.1 In some circumstances misconduct by police officers or police staff, whilst not meeting the criminal threshold for covert policing tactics under RIPA, is such that there is a positive duty for the service to act.

2.2 The Chief Constables have a duty of care to all personnel and a responsibility to ensure that confidence in the integrity of the Force is shared by the community and public. Misconduct, for example arising from incidents of unfair discrimination, engaging in sexual relationships on duty, bullying, sexual harassment, unauthorised release of information to the media etc. often requires the deployment of (redacted text) which (in the absence of criminal conduct) would fail to meet the criteria for a RIPA authorisation.

2.3 The use of covert techniques in any investigation into allegations of serious misconduct should be authorised in accordance with the appropriate legislative provisions. The [Investigatory Powers \(Interception by Businesses for Monitoring and Record-keeping purposes\) Regulations 2018](#) provides for the monitoring of all staff communications in the workplace unless subject to legal privilege. Nothing in this procedure supersedes the application of RIPA; if the circumstances of the alleged misconduct require a criminal investigation, then the relevant legislation and authority must be adhered to without exception.

2.4 The Executive Authority procedure applies to covert techniques conducted during the investigation of misconduct by police officers and police staff within the workplace, and in circumstances outside of the workplace where such misconduct relates to a breach of the Standards of Professional Behaviour, [The Police \(Complaints and Misconduct\) Regulations 2020](#), [The Police \(Conduct\) Regulations 2012](#) and staff procedures (for example, restrictions on private life, incompatible business interests etc.) or in relation to abuse of the Pension Regulations and performance and attendance management procedures.

2.5 The term 'workplace' includes any Force premises or Force-controlled vehicle, or any other place where the staff member is required to be during the course of their duty or

otherwise on behalf of the organisation. An Executive Authority will not be granted under this procedure for covert techniques in relation to any activity taking place on residential premises or in a private vehicle, other than to the extent to which people outside of the boundary of the residential premises, or outside of the private vehicle, would ordinarily be able to view.

2.6 The Forces are committed to maintaining professional standards through effective leadership. This procedure sets out the circumstances in which such techniques may be authorised by way of 'executive' rather than 'statutory' authority.

2.7 Redacted text

2.8 This procedure does not in any way preclude the use of other investigative methods, which do not require deployment of covert investigative techniques.

3. Medical Integrity Surveillance

3.1 There is also a need to manage a process where the Forces use medical integrity surveillance to ensure medical pensions and sickness absence costs are managed effectively. There is no intention to deny pension or sick pay to those staff which are genuinely ill. However, it is recognised that a small minority of people may abuse their pension and sickness rights and medical integrity surveillance is a proportionate response to such concerns.

3.2 Medical integrity surveillance will be used as a last resort where it is believed that an individual may be abusing their rights.

3.3 The use of medical integrity surveillance may be considered for example when investigating fraudulent claims for medical ill health retirement, fraudulent or false sickness absence, to evidence improvement in ill health that led to retirement but is not reported.

3.4 Prior to any surveillance taking place, the Occupational Health Unit / Human Resources / People Services may be consulted to establish whether the alleged activity is compatible with the nature of the illness or disability. Appropriate information sharing here is key to avoid unnecessary intrusion and under such circumstances the extent of any illness or disability should be appropriately shared with the ACU / PSD.

3.5 Please note that the Occupational Health Unit is bound by confidentiality under law and therefore restricted regarding the information they may be able to share.

4. Principles

4.1 Any failure by the Forces to deal satisfactorily with serious conduct matters serves only to undermine the confidence of staff and the public. The respective Force Chief Constable has a legal responsibility for the effective management of the Force, including maintenance of the highest professional standards and investigation of allegations of misconduct which may undermine the effectiveness of the organisation.

4.2 The principles of the [Human Rights Act 1998](#) must be applied when considering such applications, particularly the proportionality of the intrusion sought. The use of covert policing techniques, including surveillance and covert human intelligence sources, may engage [Article 8 Right to respect for private and family life](#). [Section 6](#) of the Human

Rights Act reinforces that it is unlawful for public authorities to act in a way that is incompatible with the rights afforded in the convention.

5. Authorisation

5.1 The use of Executive Authority is limited to investigation of misconduct or cases which are criminal but not investigated as such and would never be referred to the Crown Prosecution Service (CPS) by the Appropriate Authority and as a result will be dealt with proportionately as misconduct, where the use of covert policing techniques represents the most proportionate means of securing evidence required to determine the matter. Some matters may be referred to the Independent Office of Police Complaints (IOPC).

5.2 For this procedure, the definition of misconduct will be the same as the definition within The Police (Complaints and Misconduct) Regulations 2020, The Police (Conduct) Regulations 2012 and police staff disciplinary policies.

Police Staff Disciplinary Policy (Surrey and Sussex) (797).

5.3 During an investigation where an Executive Authority has been obtained, and criminal conduct is identified requiring continued surveillance, the Executive Authority must be cancelled, and an appropriate RIPA authorisation obtained as soon as is practicable (there is no necessity to cease surveillance while a conversion is sought).

5.4 The Authorising Officer for the purpose of Executive Authority (AO-EA) is identified as the Deputy Chief Constable (DCC), if unavailable authorisation can be delegated to the Chief Constable. The AO-EA must be satisfied that the use of the techniques being applied for represents an appropriate means of securing the evidence required to determine the matter under investigation. Use of the technique must be:

- a) Necessary
- b) Justified in the circumstances of the case.
- c) Proportionate to the seriousness of the misconduct of the application.
- d) Lawful

5.5 In the case of renewals, the AO-EA must be satisfied that grounds for the original authorisation continue to be met and that renewal of the authorisation is likely to result in achieving the objectives.

5.6 All applications for Executive Authority will be managed by the respective Forces PSD / ACU. Applications must be prepared under the supervision of an officer of at least Sergeant rank, or police staff equivalent.

5.7 Applications and authorisations will be in writing, other than in exceptional circumstances. An oral authorisation will only be made where the AO-EA considers that deployment of covert techniques in pursuance of an investigation is urgent and necessary. The authorisation will last for 72 hours and will be subject of a full written authorisation before the 72 hours elapses unless the authority is cancelled.

5.8 Information must be provided on the application to inform the decision of the AO-EA regarding legality, necessity, proportionality, and justification. Consideration should be given where there may be special sensitivities, for example, occupational health matters.

5.9 A written authorisation is valid for a period of three months (12 months for CHIS), starting with the day on which it is given, unless it is cancelled. Urgent oral authorisations are valid for 72 hours only, at which point they must be either renewed or cancelled.

5.10 The Investigating Officer must continually re-assess justification for use of the authorised techniques. Where new information has a material bearing on the grounds for the authorisation, the matter must be brought to the attention of the AO-EA by means of an interim review at the earliest opportunity.

5.11 An authorisation may be renewed for a further period, provided that the criteria for authorisation continue to be met.

5.12 An authorisation must be cancelled as soon as it is known that the grounds for continued authorisation cease to exist. A cancellation form must be completed under the supervision of an officer not below Sergeant rank or police staff equivalent and forwarded to the AO-EA.

- If a covert approach is to be considered then Regulation Notices may also be withheld and the guidance in The Police (Complaints and Misconduct) Regulations 2020, The Police (Conduct) Regulations 2012 and respective Force disciplinary policy will be followed by the ACU / PSD

Where either the harms test applies, the reasons and rationale for any delay in serving written notices or terms of reference shall be documented. When the justification that prevented service no longer applies, the relevant notice must be served as soon as practicable and duly recorded. Failure to do so can breach the regulations and may result in an abuse of process argument at a misconduct proceeding.

6. Administration

6.1 Application, renewal and cancellation forms will be retained within the PSD ACU. The form used will mirror the most current format of the RIPA forms used in criminal investigations.

6.2 The ACU will maintain a record of all applications and authorisations for the use of covert techniques under Executive Authority. All forms and other documentation must be retained and made available for inspection by the Office of Surveillance Commissioners as required.

6.3 Conventional surveillance procedures and logbooks should still be used under Executive Authority to ensure the clear documentation and retention of evidence.

6.4 There is no requirement for Executive Authority forms to go through RIPA Compliance Unit / Central Authorities Bureau or the respective Force AO however, this should not exclude tactical advice being sought from them regarding the minimisation of collateral intrusion or similar.

7. Monitoring and evaluation

7.1 The Head of Professional standards or in their absence, the Deputy Head of PSD will monitor the application and use of Executive Authority. The process will be reviewed on a regular basis by the AO-EA.

8 Related procedures, policies and information sources

8.1 Airwave Tetra (Terrestrial Trunked Radio) Technology (Surrey only)

Personal Issue of Handheld Terminals Policy (Airwave) (594) (Sussex only)

Attendance Management Policy (Surrey and Sussex) (950)

Performance and Gross Incompetence Management Policy (Surrey and Sussex) (1228)

Police Staff Disciplinary Policy (Surrey and Sussex) (797)

Lawful Business Monitoring Policy (Surrey and Sussex) (1196)

Force Issued Electronic Devices Policy (Surrey and Sussex) (1177)

The Police (Complaints and Misconduct) Regulations 2020

The Police (Conduct) Regulations 2012

Regulation of Investigatory Powers Act 2000 (RIPA)

Authorised Professional Practice (APP) Counter Corruption

College of Policing Code of Ethics

Human Rights Act 1998

Investigatory Powers Regulations 2018

Investigatory Powers Act 2016

9. Challenges and representation

9.1 Challenges / representations in respect of decisions made in applying this policy should be addressed to the Chief Constable of the relevant Force.

Team: Professional Standards Department