College of Policing

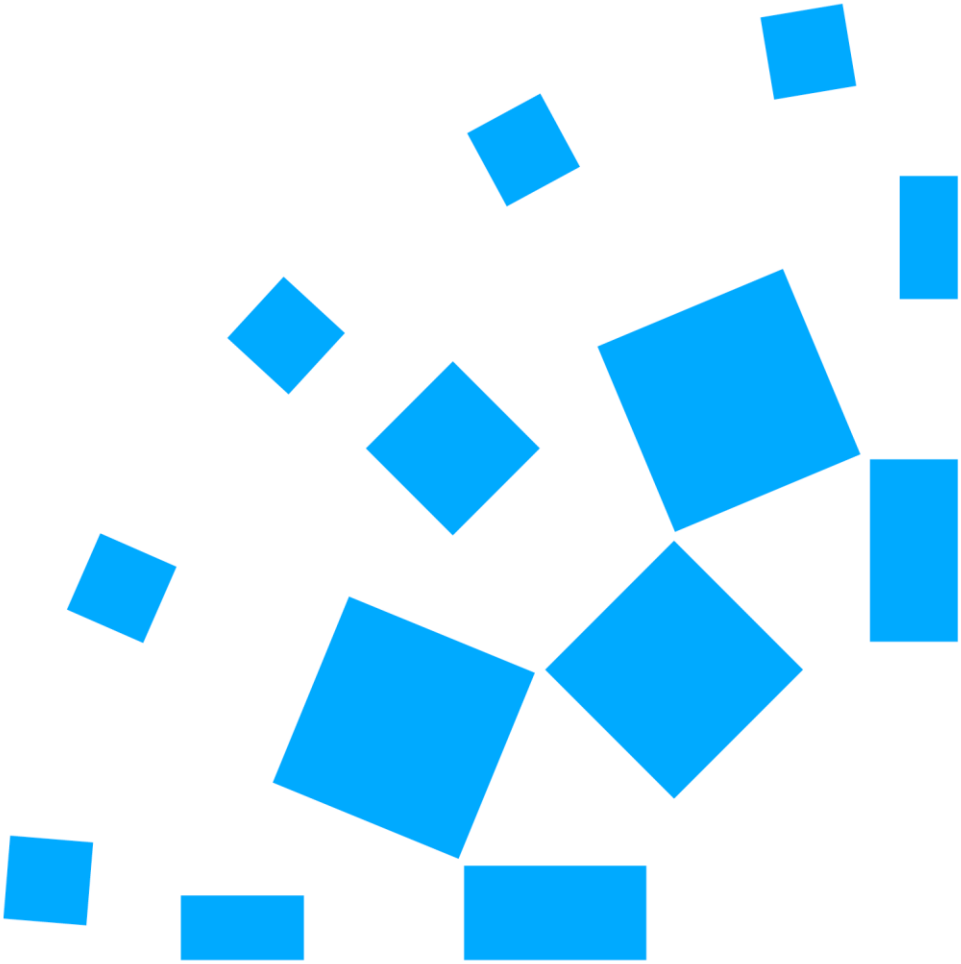
APP
AUTHORISED PROFESSIONAL PRACTICE

Working together
to keep people safe

Undercover policing

Authorised Professional Practice

October 2020



This publication is available for download at **https://www.app.college.police.uk/app-content/covert-policing/undercover-policing/**

For any enquiries regarding this publication, please contact us at the College of Policing on 0800 4963322 or email **contactus@college.pnn.police.uk**

This document has been created with the intention of making the content accessible to the widest range of people regardless of disability or impairment. To enquire about having this document provided in an alternative format, please contact us at the College of Policing on 0800 4963322 or email **contactus@college.pnn.police.uk**

Undercover policing

A number of covert tactics are available to law enforcement to prevent and detect crime or disorder and maintain public safety. Undercover is one of them.

Applied correctly and supported by appropriate training, undercover is a proportionate, lawful and ethical tactic that is effective in obtaining evidence and intelligence.

This APP applies to police forces in England and Wales. However, there is a strong collaboration between wider law enforcement agencies (LEAs) across the United Kingdom to make sure that all undercover law enforcement activity is conducted legally, ethically and safely. LEAs that are represented at the National Undercover Working Group (NUWG) have agreed to apply the contents of APP to their operations to the extent that they can. APP refers to arrangements that apply in other LEAs at various points to ensure that the principles that apply to undercover law enforcement activity are implemented consistently.

Note: Any reference to officers refers to any individual performing a designated role within an accredited undercover unit.

Contents

See also a **statement** from Chief Constable Alan Pughsley, National Policing Lead for Undercover (March 2020).

Note: this APP has been developed in conjunction with the NUWG, addressing the learning from the Undercover Policing Inquiry available at the time of publication.

1. Accreditation

The undercover accreditation process is designed to provide an objective and impartial assessment led by the College of Policing to determine whether the management and governance of undercover units are effective in supporting safe, ethical and lawful undercover operations and deployments.

Contents

1.1. Accreditation process

All units that manage undercover operations should undertake a self-assessment process for accreditation to deploy undercover operatives. Units may request accreditation under three categories: foundation, advanced, and undercover online. The accreditation level determines the activity that the unit can carry out.

The process follows a three-year cycle as detailed below.

1.1.1. All units complete a self-assessment

Self-assessment describes the undercover authorisation, governance and tactical management arrangements units have in place. The descriptions set out how units manage foundation, advanced and online undercover activity.

Self-assessments are submitted to the College of Policing Accreditation Registrar who will assess and make a recommendation to the accreditation panel. A panel will be convened to review the Registrar's recommendations and to award provisional accreditation.

1.1.2. Accredited units update and certify their self-assessments

Units should update their self-assessments when significant changes occur to their structure or operating practices and certify the accuracy of assessments annually.

1.1.3. Accredited units are visited by College of Policing validators at least every three years

Validators will make recommendations to the College of Policing accreditation panel about whether the unit should continue to be accredited or whether the accreditation should be amended or withdrawn.

1.1.4. The College of Policing panel reaccredits units based on the outcome of validation visits

The content of annual self-assessments, or failure to submit annual updates, may trigger a validation visit or cause accreditation to be withdrawn. If the accreditation registrar becomes aware of concerns about a unit’s performance, they may arrange a validation visit or withdraw accreditation with immediate effect.

A panel will be convened to review the registrar's recommendations and to award full accreditation.

Units can also receive practical advice and support from the NUWG.

1.2. Oversight and governance

The following organisations provide oversight and governance to undercover:

- **College of Policing**
- **Investigatory Powers Commissioner's Office (IPCO)**
- **Investigatory Powers Tribunal**
- **Crown Prosecution Service (CPS)**
- **Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services**
- **National Police Chiefs' Council (NPCC) through oversight from the NUWG**

See also the authorising officer and senior responsible officer role descriptions in chapter 3.

2. Undercover operatives

Undercover operatives (UCOs) are deployed under direction in an authorised investigation or operation as a **covert human intelligence source** (CHIS).

The Regulation of Investigatory Powers Act 2000 defines a person as a CHIS if:

a. they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

b. they covertly use such a relationship to obtain information or to provide access to any information to another person; or

c. they covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Statutory Instrument 2013/2788 further defines a UCO as a **relevant source** holding an office, rank or position with the public authorities listed in the order and Annex B of the CHIS Code of Practice (2018).

Relevant sources have enhanced authorisation arrangements as detailed in the **CHIS (2018) Revised Code of Practice**.

The NUWG defines a UCO as a specially trained law enforcement operative working under direction in an authorised law enforcement operation in which the operative's identity and purpose is concealed from third parties.

For further information, see chapter 7 Conduct and chapter 8 Authorisation process.

UCOs volunteer for selection, vetting, training and accreditation. Once in post they must comply with the Undercover (UC) Code of Conduct as well as the College of Policing Code of Ethics, which applies to all police officers. The length of time in post may vary in line with the College of Policing **risk-based tenure guidance**.

At the time of publication, the foundation programme was the single point of entry for staff seeking to become a UCO – however, direct access to advanced level is being developed.

Anonymity is fundamental to maintaining the ongoing safety and welfare of UCOs, and must be considered in all proceedings involving UCOs.

Contents

2.1. Categories of UCO

There are three categories of UCO:

- undercover **foundation** operatives (UCFs)
- undercover **advanced** operatives (UCAs)
- undercover **online** operatives (UCOLs)

Qualified UCFs or UCAs can work online but those qualified as UCOLs only are restricted solely to online deployments.

There are robust selection, training and development processes for staff who undertake the UCO role.

2.1.1. Foundation operatives

UCFs carry out deployments that do not require significant backstopping. Backstopping is the process of establishing and maintaining documentation and facilities that support covert identities and structures capable of withstanding scrutiny.

After initial training, UCFs can attain additional modules that enable them to be deployed on a greater range of duties. For example, online or street drug buyer.

UCFs undertake continuing professional development (CPD) to maintain their accreditation and so they can be deployed in specialist subject areas. UCFs can be deployed with UCAs, but only in supporting roles.

2.1.2. Advanced operatives

UCAs are trained to undertake deployments where a significant level of backstopping is required.

UCAs undertake CPD to maintain their accreditation and to allow their deployment in specialist subject areas.

2.1.3. Online operatives

Online investigations cover a wide range of deployment types.

Tactics employed include daily research by officers carrying out covert network exploitation and infiltration tactics deployed by UCOs.

UCOLs can be either foundation or advanced UCOs appropriately trained to operate online, or can be dedicated to work online only as an undercover online operative only (UCOLO).

2.2. Eligibility to deploy

A UCO's/UCOLO's status can change over time. To be deployable, a UCO/UCOLO must be deemed to be **active**.

Absence of any of the qualifying criteria in the active status category will result in the UCO/UCOLO being recorded as **dormant**.

Dormant UCOs/UCOLOs require an individual development plan before they can be deemed active. This development plan and their return to active status should be endorsed by the covert operations manager for undercover (COM-UC).

2.2.1. Qualifying criteria

The qualifying criteria for active status differ for UCFs, UCAs and UCOL/Os:

Active status is achieved by satisfying the following	**UCF**	**UCA**	**UCOL/ UCOLO**
Deployed in the last 12 months or Undertaken CPD (local, role-specific and national) in the last 12 months	✓	✓	✓
Signed the UCO code of conduct on an annual basis	✓	✓	✓
Been subject to regular psychological assessment – every three months for those deployed in very stressful roles, such as investigating online child abuse; every six months for advanced operatives; on a risk basis for UCFs, depending on the nature of deployment and the risks of harm s/he may be exposed to	As required	Every six months	Every three months
Supported by the respective COM-UC	✓	✓	✓

2.3. Tenure and reintegration

A fixed-term tenure cannot meet the needs of all undercover units and operatives. Instead, UCOs are assessed by their COM-UC according to a risk-based tenure policy developed by the College of Policing and applied by the NUWG.

See **Tenure and reintegration guidance** for further information.

2.4. UCO training pathways

The College of Policing licenses all undercover selection processes and undercover training courses. Selection and training are delivered to national standards by subject matter experts who have received training, and hold qualifications to carry out their roles as recognised by the College.

UCOs may undertake a number of training paths.

- Foundation programme – UCF
- Advance programme – UCA
- Online element – UCOL
- Online only – UCOLO

3. Infrastructure

To deliver the undercover tactic, accredited units require the following functionality:

Contents

3.1. Cover officer

Cover officers are responsible for UCOs' security and welfare. They ensure interactions between the UCO and the operational team happen in accordance with agreed sterile corridor arrangements so that there is no uncontrolled contact between the two.

Cover officers are independent of the operational team and work under the direction of the undercover unit while undertaking cover officer duties. See **section 29(5)(a)/29(4A)(a)** of RIPA and section 7(6)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA).

Officers must have attended and passed the national cover officer course to undertake this role. Cover officers should be fully conversant with current law, procedures and guidelines relevant to undercover operations. This includes disclosure and revelation issues.

Where a UCO is donated by a law enforcement agency, the donor unit should allocate a cover officer to act as a conduit between the host cover officer and the donor unit. See paragraph 4.8 on host and donor units.

3.1.1. Legal requirement

- Dealing with the UCO on behalf of the law enforcement agency.
- Directing the day-to-day activities of the UCO.
- Ensuring the UCO accurately records details of their deployment.
- Monitoring the UCO's security and welfare.

3.2. Backstopping

The backstopping function maintains pseudo-identities.

Pseudo-identities help preserve the true identity of a UCO and/or covert premises, maintain a UCO's legend and help minimise the risk of compromise.

Backstopping is managed by a nominated person who is the single point of contact (SPOC) responsible for all backstopping issues. This role includes maintaining operational security in conjunction with the operational security officer (OPSY).

3.3. Office and administration support

Office and administration support should be commensurate with the requirements of the unit at a given time.

3.4. COM-UC

The COM-UC is an officer of at least inspector rank, or equivalent, who is responsible for the management and supervision of the UCO (see RIPA **section 29(5)(b)** or section 7(6)(b) RIPSA). The COM-UC is responsible for the day-to-day running of the undercover unit.

The COM-UC is the decision-maker regarding the covert tactics and tasking undertaken by UCOs. These decisions will be within the parameters of the authorisation granted by the authorising officer.

The COM-UC must have attended and passed the COM-UC course to undertake this role. The COM-UC should be fully conversant with current law, procedures and guidelines relevant to undercover operations. This includes disclosure and revelation issues.

3.5. Head of unit

The head of an undercover unit is an officer of at least chief inspector rank or equivalent. They are responsible for the overall management, strategic direction and development of the undercover discipline.

3.6. Operational lead

The operational lead is an officer of at least inspector rank or equivalent. They manage the investigation or operation in which the UCOs are deployed and set the operational objectives.

At the commencement of and for the duration of an operation, the operational lead should consult the undercover unit and agree the approach. This is to make sure the approach fits operational objectives.

Operational leads should not be attached to the undercover unit nor be the line manager of deployed UCOs. They should be aware of current legal issues and guidelines relevant to undercover operations.

3.7. Authorising officer

The authorising officer (AO) is an officer of at least assistant chief constable rank or equivalent. They are the person responsible for granting the use and conduct of UCOs. Where the UCO has been deployed for a cumulative period of longer than 12 months, or where there is a likelihood of obtaining confidential or privileged information, the AO will be a chief constable or equivalent and require the prior approval of a **judicial commissioner**.

Responsibility for authorising the use or conduct of a CHIS rests with the AO and all authorisations require the personal authorisation of the AO. The Regulation of Investigatory Powers (Directed Surveillance and CHIS) Order 2010, as amended by the Regulation of Investigatory Powers (CHIS: Relevant Sources) Order 2013, designates the AO for each different public authority and the officers entitled to act only in urgent cases. (5.6 CHIS Code of Practice 2018 and **SI 2788**).

AOs must have attended and passed the College of Policing's Authorising Officer course prior to undertaking this role.

See also chapter 8 Authorisation process.

Please note: The Regulation of Investigatory Powers (Directed Surveillance and CHIS) Order 2010 is later referred to throughout this APP as the CHIS Order), and the Regulation of Investigatory Powers (CHIS: Relevant Sources) Order 2013 is referred to as the Relevant Sources Order.

3.8. Senior responsible officer

The senior responsible officer (SRO) is a designated person in each organisation who is responsible for:

- the integrity of the process in place within the police force or public authority for the management of UCOs
- compliance with Part II of RIPA and the Covert Human Intelligence Source Codes of Practice
- oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors

- engagement with the IPCO and inspectors who support the Commissioner when they conduct their inspections
- where necessary, oversight of the implementation of post-inspection action plans recommended or approved by the IPCO
- ensuring that all AOs are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the IPCO. (9.1 CHIS Code of Practice, 2018).

4. Welfare

UCOs require a safe, secure and confidential environment to receive psychological assessment and mental wellbeing support from qualified practitioners.

Contents

4.1. Assessments

There are two types of UCO assessment that address psychological suitability for the role(s):

- personality assessment (selection for UCF)
- psychological assessment (selection for UCA and UCOLO)
- personality and psychological assessment for selection for direct access to UCA training.

4.2. Personality assessments

Candidates going through the foundation selection process undergo a personality assessment with an occupational psychologist who is provided by the College of Policing. This assessment helps identify the personal characteristics relevant to the requirements of the role.

The personality assessment evaluates a candidate's motivation, suitability and resilience for the UCO role. It does this by identifying areas of strength and potential areas of concern that may require further exploration during the assessment process.

4.2.1. Personality assessment practitioners

Practitioners of personality assessments (selection) must hold an MSc in occupational psychology with several years' experience of using and applying personality measures for selection and assessment.

Practitioners must be approved by the College of Policing and have received College training regarding the process and expectations of the role. All practitioners should be vetted to security check (SC) level.

Personality assessment practitioners:

- **work** with the College of Policing (and other personnel as appropriate) to ensure the most effective and accurate personality assessment following a one-to-one meeting with the UCO
- **give** written reports to the College and forces/agencies to inform selection processes
- **follow** guidance and processes as laid out by the College

4.3. Psychological assessments

UCOs receive psychological assessment under two areas:

- selection and readiness
- ongoing assessment

4.3.1. Selection and readiness

UCOs are subject to a psychological assessment for **selection** as follows:

- advanced selection process
- online only selection process

UCOs are subject to psychological assessment to ensure **readiness** as follows:

- online module – UCOs should not undertake the online module without first ensuring they are psychologically prepared to undertake the role.

Psychological assessment is a semi-structured one-to-one interview session with a qualified practitioner (a chartered clinical psychologist or registered psychiatrist).

This assessment ascertains whether there are any psychological factors that may present a risk to the candidate's wellbeing, their performance in training or their suitability to undertake advanced and/or online work. It also identifies positive factors indicating suitability for deployment.

Following the psychological assessment for selection, a brief report is produced by the practitioner for the selection assessment team. With regard to readiness for online work, the COM-UC should receive the ongoing report from the practitioner and discuss if any issues are raised.

4.3.2. Ongoing assessment

Active UCOs are subject to ongoing psychological assessment as follows:

- undercover foundation operatives (UCFs) – at the direction of the relevant COM-UC
- undercover advanced operatives (UCAs) – every six months – to be reviewed by the COM-UC in line with the nature of the deployment

- undercover online operatives (UCOLs) and undercover online only operatives (UCOLOs) – at least every three months. This is a risk- and individual-based approach at the discretion of the COM-UC. UCOLs are subject to assessment every three months because the nature of their work is often intensive, moving from one engagement to another in succession and often in highly stressful and/or unpleasant settings, such as online child abuse. Where deployments are not so demanding, COM-UCs may decide to adopt a risk-based approach that meets the deployment needs of the UCOL

Ongoing assessments are carried out by a qualified practitioner (chartered clinical psychologist or registered psychiatrist). The aim of these ongoing assessments is to ascertain whether there are any psychological factors that may present a risk to the UCO's wellbeing or to the effectiveness and safety of any operation on which the UCO may be deployed.

Ongoing assessments can also identify the presence of positive factors indicating suitability for particular deployments.

Ongoing assessments also give consideration to the potential psychological impact that issues related to online work such as frequently viewing graphic and disturbing images can have on operatives.

Before a psychological assessment of a UCO, the COM-UC can, at their discretion, communicate with the clinical psychologist or psychiatrist. The purpose of this communication is to ensure that the psychologist or psychiatrist understands the unique features of the deployment(s), and any relevant information about the UCO, which may affect their fitness for the role.

4.3.3. Psychological assessment practitioners

Practitioners of psychological assessments (selection and ongoing) must be chartered clinical psychologists registered with the Health & Care Professions Council or psychiatrists registered with the General Medical Council.

All practitioners should be vetted to SC level or equivalent. It is the responsibility of the units to ensure practitioners are vetted.

Practitioners are directly employed by each unit but should also receive specific training and support from the College of Policing.

Psychological assessment practitioners:

- **work** with the COM-UC (and other personnel as appropriate) to ensure the most effective and accurate psychological assessment of the UCO and the most effective support and treatment, where appropriate
- **give** written and verbal reports to the COM-UC to help with decisions about fitness to deploy, selection and UCO deployments
- **provide** appropriate guidance on resilience and coping strategies to prevent psychological crises or ill health from developing
- **make** recommendations for support or treatment as appropriate, in consultation with the COM-UC and appropriate wellbeing support providers
- **follow** guidance and processes as laid out by the College

4.4. Confidentiality

UCOs should be made aware that practitioners are obliged to inform the relevant undercover unit, force or agency if they have concerns about the wellbeing or safety of the UCO, other staff or members of the public, or about the ethics or legality of UCO activities.

This policy is in line with the UCO code of conduct that requires UCOs to take personal responsibility for maintaining their mental wellbeing and informing managers of anything that may affect their fitness to operate.

The practitioners utilised by each undercover unit are also bound by confidentiality and will ensure all material is stored or retained securely at all times.

4.5. Support

Mental wellbeing support is the therapy or treatment that may be recommended following psychological assessment. The purpose of such support is to address any psychological difficulties the UCO may be experiencing and provide an up-to-date record for the COM-UC.

Practitioners who provide this support function may come from a wider range of professional backgrounds (for example, counsellors or cognitive behavioural therapy specialists). Practitioners may be found externally to the organisation or through the organisation's own occupational health team. They should be registered and accredited by an appropriate professional body and vetted to an appropriate level.

Occupational health departments may provide support or assessment if their staff have the appropriate qualifications and training (see paragraph 4.3.3). However, they should not provide both assessment and support for the same UCO.

Practitioners who provide the psychological assessment function may also provide a mental wellbeing support function (if they are suitably qualified). But, again, they should **not** do so for the same UCO they provide assessment for. This is to prevent a conflict of interest whereby the person recommending treatment is also the person providing that treatment.

4.6. Occupational health

Units must engage with their relevant occupational health department about the health and wellbeing of UCOs according to local protocols.

Where UCOs have additional roles outside the unit or on leaving the unit, COM-UCs should have due regard to any risks that the UCO may be exposed to or may present.

COM-UCs should also make sure that the appropriate personnel are informed so that such risks can be managed. This may be within occupational health or other appropriate departments.

4.7. Welfare responsibilities

COM-UCs are responsible for arranging psychological assessment and mental wellbeing support for UCOs.

Every undercover unit should have a formal system for assessment and support that follows College of Policing guidance. College of Policing guidance is based on the National Policing Improvement Agency report that identified the UCO role as encompassing high degrees of stress. There may be other roles which result in

higher levels of police work-related stress and which the COM-UC may consider need psychological support. This support includes:

- **providing** assessments by suitably qualified and experienced practitioners
- **ensuring** assessment providers have a contract with each unit and clearly defined terms of reference covering the purpose, approach, outcomes, referrals and arrangements for the security of records
- **ensuring** all confidential records are stored securely with controlled access in line with local security guidance
- **providing** a defined, confidential reporting mechanism for all officers and staff in the unit to highlight issues of concern and grounds for withdrawing UCOs and cover officers from operations
- **providing** a mechanism for the COM-UC to feed concerns about UCOs to the psychologist/psychiatrist and vice versa
- **creating** a climate that supports openness, honesty and positive regard for UCO wellbeing
- **providing** leadership that creates a culture where seeking internal and external support is regarded positively
- **ensuring** local policies underpin wellbeing and psychological support where appropriate
- **monitoring** the effectiveness of UCOs and cover officers, both as individuals and as a partnership
- **ensuring** there are appropriate protocols and policies for creating the right conditions to support UCO wellbeing (for example, that consider periods between deployments and ensure there are exit strategies)
- **ensuring** procedures exist for self-referral, required referral and routine psychological assessment with practitioners
- **ensuring** other undercover unit staff are subject to psychological assessment and mental wellbeing support as necessary
- **making** decisions, in conjunction with the cover officers and UCOs, about which deployments are particularly demanding or especially psychologically challenging and, therefore, require more frequent psychological assessments

- **ensuring** operatives have clarity on and plans for reintegration into other law enforcement roles
- **ensuring** continued welfare support for operatives after return to other duties
- **ensuring** records are kept and maintained
- **ensuring** there are links with local occupational health and other support services
- **considering** the psychological needs of others connected with the UCO, drawing on legal advice and advice of psychologists

4.8. Host and donor units

The **host** undercover unit is the unit that supports the operational lead and investigation team in providing undercover tactics. Sometimes UCOs are donated from other undercover units to support operations. In such cases, the donating UCO's undercover unit is referred to as the **donor** unit.

The cover officer in the host unit conducts ongoing reviews with all UCOs to assess their wellbeing and performance. The host cover officer maintains regular contact with the donor cover officer regarding the UCO's security and welfare. If there is cause for concern and either cover officer believes that the UCO requires psychological assessment, this will be arranged via the donor COM-UC.

Where a COM-UC in the host unit has a concern about a UCO and wishes to make a referral for psychological assessment, they should arrange this via the COM-UC of the donor unit.

If mental wellbeing support is required (for example, counselling), this will be provided by the donor COM-UC using qualified practitioners who are appropriately vetted. The donor COM-UC is responsible for ensuring that all UCAs and UCOLs attend ongoing psychological assessments, as appropriate.

5. Backstopping and legend building

Backstopping and legend building are mutually supportive processes designed to develop, maintain and support covert identities and structures capable of withstanding scrutiny.

Contents

5.1. Backstopping: purpose and process

Backstopping is the process of establishing and maintaining documentation and facilities that support covert identities and structures capable of withstanding scrutiny.

All UCOs, COM-UCs, cover officers and some support staff require a level of covert backstopping commensurate with the role they are expected to perform.

All requests for backstopping and supporting documentation should be approved by a superintendent or equivalent and processed via the undercover unit's backstopping officer.

5.2. Backstopping: support provisions

Undercover support provisions should:

- be fully backstopped, with no reference to law enforcement activity
- include premises that are fit for purpose with:
  - protocols for visitors
  - external security
  - no external identifiers
  - secure communications
- provide sufficient backstopping for UCOs to effectively service their needs in-role
- make sure there are fully supported and up-to-date legends that can withstand intrusive scrutiny
- include business continuity plans

5.3. Backstopping: covert documents

All UCOs, COM-UCs, cover officers and some support staff should have covert documentation commensurate with their needs.

Unless in exceptional circumstances, staff should not have more than one set of documentation in their physical possession. This is to prevent the risk of compromise.

Covert documentation should be issued and stored in accordance with local procedures when not being used.

5.4. Legend building: initial planning

Legend building is a process whereby a UCO carries out covert activity which may include visiting or frequenting a location, for the purpose of developing a covert history or covert identity. It is a necessary means of developing cover stories and legend to maintain credibility in role.

UCOs engage in legend building activity that is commensurate with their role (UCA, UCF, and UCOLO).

Initial planning should involve contacting the relevant undercover unit(s) where appropriate. This is the responsibility of the COM-UC. This is to understand any particular sensitivities in the local community where the UCO is to conduct legend building activity and be aware of similar activities being undertaken by other public authorities which could have an impact on deployment.

Contact must always be made with the undercover units in the Police Service of Northern Ireland and Police Scotland when planning to legend build in Northern Ireland and Scotland respectively.

5.5. Legend building: approval not to authorise

When a UCO is deployed to build up their legend, an authorisation should be considered under the RIPA if the activity will interfere with an individual's Article 8 rights. This will include circumstances where it is not clear to individuals with whom the UCO may come into contact that the UCO is not who he or she claims to be. The individual does not have to be the subject of any current or future investigation. Interference with any individual's Article 8 rights as part of legend building should be authorised under the RIPA. When an authorisation is not considered necessary, arrangements should be in place to maintain active review of this position, and any decision not to authorise should be made by the person prescribed to act as the AO. (Section 2.16 CHIS Code of Practice, 2018)

All legend building deployments must be approved in advance of activity.

The **IPCO** has acknowledged that some legend building activity, where the criteria for an authorisation under the RIPA are not met, may not require authorisation. In these cases, an AO approval must be obtained from an assistant chief constable or equivalent who has been trained as an AO (in these circumstances they will become an approving officer).

Requests for legend building activity will be considered by the COM-UC before they are presented to the approving officer. The COM-UC should be satisfied that:

- the legend building plan is appropriate
- collateral intrusion must be continually reviewed and managed.
- risk associated with such activity must be continually reviewed and managed

If legend building activity exceeds or is likely to exceed 12 months, approval remains with the approving officer at assistant chief constable level or equivalent. Legend building approvals should be reviewed at the direction of the AO approving the activity.

5.6. Legend building: evidence and intelligence

Prior to deployment, the cover officer will ensure that UCOs undertaking legend building activity understand they may be required to give evidence in court if they inadvertently obtain information. Records must always be maintained to an evidential standard.

Building a legend specifically to be used on an identified operation requires RIPA authorisation.

6. Operational security

The undercover discipline requires a high level of operational security to minimise risk and operate effectively.

Secure systems are critical to the integrity of the undercover unit, its staff and operations.

Contents

6.1. Security responsibilities

The COM-UC is responsible for overall security, but all staff have a role to play in identifying security issues and adhering to security policies.

The operational security of the undercover unit, including its interactions with the operational team, is achieved and maintained by:

- ensuring all staff undergo appropriate vetting
- ensuring all identified security risks are assessed and documented and that there are appropriate risk management measures – this requires consultation with an operational security officer
- ensuring need-to-know principles are adhered to by all staff and operational teams in relation to UCOs and associated operations
- using and managing indoctrination agreements so that anyone interacting with the unit or staff understands security arrangements
- managing asset security
- managing all security-related elements of IT and communications
- applying **Government Security Classification Policy (GSCP)** requirements
- ensuring all confidential records are stored securely with controlled access in line with local security guidance
- ensuring continuous deconfliction of operations
- referring and reporting to national databases as appropriate
- ensuring liaison with local or regional freedom of information (FOI) teams and coordinating responses to FOI requests nationally
- ensuring a media strategy is in place to protect individuals and covert tactics
- restricting awareness of sensitive sources and covert methods on a need-to-know basis
- briefing the operational lead on the need to protect covert methods and terminology to be used with the media and in prosecution reports
- ensuring audio/visual product and other evidential material is managed effectively and ensuring protocols are in place on handling, copying and using audio/visual product and other evidential material in any prosecution case.

Clear separation must be maintained between those responsible for the investigation and those managing the UCO to ensure the welfare and safety of the UCO are always given due consideration.

6.2. Vetting

Undercover unit personnel should be cleared to Management vetting, with SC only applied where the post holder requires long-term, frequent and uncontrolled access to government assets marked as SECRET. Heads of units, COM-UCs and psychologists should hold a minimum of SC clearance. Other professionals and force employees should be vetted in line with **APP on vetting**.

6.3. Sensitive source intelligence

Intelligence from sensitive sources should be managed securely and suitably sanitised for dissemination using an **intelligence report**.

Sterile corridors must be established and maintained by all staff for the receipt of all sensitive intelligence. COM-UCs will consult the sensitive intelligence network.

6.4. Freedom of information and data protection requests

A force receiving a request for information relating to undercover policing issues under the Freedom of Information Act should consult the National Police Freedom of Information & Data Protection (NPFDU) Central Referral Unit (CRU) for advice, at **npcc.advice@cru.pnn.police.uk**

The NPFDU manages advice to forces on behalf of the NPCC, which maintains communication with the NUWG.

Additionally, if information is held, consultation will be necessary with the NPCC FOI Officer & Decision Maker who manages NPCC FOI requests on behalf of the NPCC, to ascertain whether the NPCC wishes to propose the engagement of any exemptions. In this case, contact the NPCC FOI Mailbox: **npcc.foi.request@cru.pnn.police.uk**

Where subject access requests (SARs) are made to forces, the force Data Protection Officer (DPO) will advise the NPFDU Data Protection Advisor (DPA) at **data.protection@npcc.pnn.police.uk** to ensure the NUWG is consulted.

6.5. Media strategy

Operations involving undercover tactics may attract the interest of the media. It is essential this interest is managed appropriately to safeguard ongoing and/or future activity.

The disclosure and subsequent reporting of the use of UCOs in any court proceedings cannot be avoided; reporting restrictions can be considered only in exceptional circumstances and only ordinarily where there are other linked and un-finalised cases.

The fact that UCO activity becomes known to the press through courtroom reporting does not alter the position around neither confirm nor deny (NCND) (See paragraph 6.5.1).

No information will be passed to the media that might lead to any of the following (even if they have been referred to in court or elsewhere in the public domain):

- identification of UCOs or CHISs
- how the management of covert tactics and methods are applied
- revelation of the existence or details of particular items of technical equipment

Although various publications and television programmes may describe covert tactics, law enforcement agencies should not endorse such exposure.

There may be cases where it is deemed beneficial to reference the use of UCOs in media releases. This should be agreed by the COM-UC on a case-by-case basis.

Any requests from media or other organisations to take part in fly-on-the-wall type programmes depicting the use of undercover techniques must be referred to the NUWG.

Any requests from partners (including, for example, law enforcement, academia and voluntary organisations) which may expose information detailed in the bullet points above must be referred to the NUWG.

6.5.1. Neither confirm nor deny

The established principle of NCND is used by law enforcement agencies to protect covert methods, sensitive information and the identity of sources of information including UCOs.

NCND is not to be used to hide information the force or agency does not wish to disclose. It safeguards tactics and the lives and wellbeing of UCOs, their families and others.

Sometimes simply confirming or denying whether a force or agency holds a particular category of information could itself disclose sensitive and damaging information. The principle of NCND is needed to prevent harm which may arise if law enforcement agencies have to confirm or deny whether they hold particular information. Specifically:

- to confirm that a person is a UCO would place that person in immediate and obvious danger
- to deny that a person is a UCO may place another person in immediate and obvious danger
- to comment either way in one case raises a clear inference where there is a refusal to comment in another case that there is something to hide in that case

The local police force or law enforcement agency communications office can help handle media enquiries. In cases of difficulty, the **NPCC media office** can advise.

6.6. Social media

All undercover unit staff should be aware of the dangers posed through exposure of their true identity on social media networks, as this may undermine the covert nature of their role.

All undercover unit staff have individual responsibility to ensure that their covert identity is protected online.

Any individual who compromises themselves, colleagues, operations or covert assets by using social media may be subject to disciplinary procedures. Any exposure will be subject to a thorough risk assessment by the COM-UC, with referral to the SRO in cases where significant risks to individuals or the unit arise.

7. Conduct

UCOs remain bound by the laws, rules, regulations and codes governing law enforcement agencies.

The AO should consider any conduct likely to have a negative impact on the health and wellbeing of UCOs and this should be mitigated in the relevant risk assessments.

For further information, see:

- College of Policing Code of Ethics
- CHIS (2018) Revised Code of Practice
- National Code of Conduct for Undercover Operatives

Contents

7.1. Agent provocateur

Agent provocateur has been defined as a person who entices another to commit an express breach of the law that they would not otherwise have committed and then proceeds to inform against them in respect of such an offence. (Royal Commission on Police Powers and Procedures (1929)).

A UCO must not act as an agent provocateur.

7.2. Parameters

Any application for the use and conduct of a UCO should make clear the precise parameters of the UCO's conduct. Authorised conduct may differ between UCOs, including between UCOs deployed on the same operation. The cover officer, COM-UC and operational lead will ensure that specific tasking of operatives remains within the parameters of the authorised conduct.

7.3. Participation in criminal activity

For an undercover deployment to be effective, it may be necessary for UCOs to participate in the criminal activity about which they have been tasked to report. Case law has recognised the requirement of UCOs to participate in criminal activity and has identified the limits of acceptable law enforcement conduct (R v Loosely [2001] UKHL 53). This will be set out as part of the conduct specified in the RIPA authorisation.

See section **225.5 Office of Surveillance Commissioners (OSC) guidance (2016)** for further detail.

AO considerations in granting such an authorisation include that UCOs:

- do not actively engage in planning and committing the crime
- are intended to play only a minor role
- participate only where essential to enable law enforcement to frustrate the principal criminals and arrest them (albeit for lesser offences such as attempt or conspiracy to commit crime, or carrying offensive weapons) before injury is done to any person or serious damage is done to property

7.4. Use of equipment by a UCO

The UCO wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the UCO. However, if a surveillance device is to be used other than in the presence of the UCO, an intrusive or directed surveillance authorisation should be obtained where appropriate, together with an authorisation for interference with property, if applicable. (See **3.25 CHIS Code of Practice**, 2018.)

A UCO, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations or other forms of communication that takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way. (See 3.26 CHIS Code of Practice, 2018.)

If a UCO is acting on behalf of one of the bodies to which the equipment interference provisions of the Investigatory Powers Act 2016 apply, and is required as part of his or her tasking to interfere with equipment in order to obtain communications, equipment data or other information, that interference should be authorised separately by a warrant under that Act. (See 3.27 CHIS Code of Practice, 2018).

7.5. Intimate and sexual relationships

It is never acceptable for a UCO to have an intimate sexual relationship with those they are deployed to infiltrate and target or encounter during their deployment. Having an intimate sexual relationship must not be used as a tactic by a UCO.

If a UCO engages in an intimate sexual relationship (for example, they perceive an immediate threat to themselves and/or others if they were not to do so) this activity will be restricted to the minimum conduct necessary to mitigate the threat. UCOs **must** record and report this to the cover officer and COM-UC immediately.

The AO must be informed immediately by the COM-UC. The circumstances must be investigated and the facts reported to the AO. The AO must consider whether the operation should continue. Referral to oversight and governance bodies must be considered where appropriate.

Conduct may be authorised for **communications** of a sexual nature to take place (for example, online) where the AO believes it is necessary and proportionate to achieve specific operational objectives, having taken into account any risk of collateral intrusion. Collateral intrusion is the risk of interference with the private or family life of persons who are not the intended subjects of the UCO activity. The parameters of the authorised conduct must be precisely documented by the AO, and must be subject to frequent and robust reviews.

If a UCO engages in unauthorised communications of a sexual nature (for example they perceive an immediate threat to themselves and/or others if they were not to do so) this activity will be restricted to the minimum conduct necessary to mitigate the threat. UCOs **must** record and report this to the cover officer and COM-UC immediately.

The AO must be informed immediately by the COM-UC. The circumstances must be investigated and the facts reported to the AO. Referral to oversight and governance bodies must be considered where appropriate.

8. Authorisation process

The use and conduct of a UCO, when regarded as a relevant source, is subject to individual authorisation under RIPA.

Contents

8.1. Introduction

Authorisations must comply with RIPA (and any other relevant legislation), and have regard for the **CHIS Code of Practice** and case law.

The COM-UC must (in consultation with the operational lead) ensure that operational and personal risk assessments have been completed before any authorisation or approval is considered.

Forms for authorisations, reviews, renewals and cancellations may be submitted to the AO by way of an electronic system or in hard copy. All records relating to authorisation processes must be retained.

8.2. Applications

The role of the applicant is to present the facts of the application for use and conduct: the crime to be investigated; the reason why it is proposed to conduct the investigation covertly; what covert tactics are requested and why; the focus of the conduct; who else may be affected by it and provide an outline of the tactical plan.

To assist the AO's assessment of proportionality the applicant should provide evidence and intelligence, but it is not the role of the applicant to establish that it is necessary and proportionate; that is the statutory responsibility of the AO.

Each application will have a unique reference number and must be accompanied by a personal risk assessment for each UCO.

The UCOs should be individually identified from the outset by their national index number and relevant suffix.

A single application may be used to authorise more than one UCO, provided operatives are individually identified, and their individual conduct clearly specified.

8.2.1. Application documents

Application documents should include:

- an application for an authorisation
- a risk assessment for each operative to be deployed
- an authorisation or refusal

- oral application and authorisation, where appropriate

Also consider including:

- any appropriate comments from the IPCO
- advice from the prosecutor
- any relevant overseas documentation

The completed application and accompanying documentation should be submitted through the Central Authorities Bureau of the relevant agency prior to consideration by the AO.

8.3. Necessity, proportionality and collateral intrusion

Necessity

The RIPA stipulates that the AO must believe that an authorisation for the conduct or use of a UCO is necessary in the circumstances of the particular case for one or more of the statutory grounds in **section 29 (3) of RIPA** (see section **5.1 of CHIS Code of Practice, 2018)**.

Proportionality

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the use or conduct of a CHIS proportionate. Similarly, an offence may be so minor that any deployment of a CHIS would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. (**3.4 CHIS Code of Practice, 2018**.)

The following elements of proportionality should therefore be considered (**3.5 CHIS Code of Practice, 2018**):

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others

- whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented, or have been implemented unsuccessfully
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought

Collateral intrusion

Before authorising the use or conduct of a source, the AO should take into account the risk of interference with the private or family life of persons who are not the intended subjects of the UCO activity (collateral intrusion). (**3.9 CHIS Code of Practice, 2018**.)

Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved.

Measures should be taken, wherever practicable, to avoid or minimise interference with the private or family life of those who are not the intended subjects of the UCO activity. (**3.10 CHIS Code of Practice, 2018**.)

Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral intrusion is considered proportionate to the aims of the intended intrusion. Any collateral intrusion should be kept to the minimum necessary to achieve the objective of the operation.

Consideration should be given to three categories of collateral intrusion referenced in the 2012 Her Majesty's Inspectorate of Constabulary Review of the national police units that provide intelligence on criminality associated with protest:

- inevitable intrusion (such as into the privacy of intimate associates of the subject)
- foreseeable intrusion (such as into the privacy of unknown associates)

- general intrusion (such as into the privacy of other members of the public who come into contact with the subject)

Where UCO activity is deliberately proposed against individuals who are not suspected of direct or culpable involvement in the matter being investigated, interference with their private and family life should not be considered as collateral intrusion but, rather, as intended intrusion and authorised as appropriate. Any such interference should be carefully considered against the necessity and proportionality criteria as described above.

Operatives from international law enforcement agencies may be authorised under RIPA to support domestic and international investigations or operations.

Consideration should be given to authorising operatives from foreign agencies at the level prescribed by **Statutory Instrument 2013/2788**, as if the individuals hold an office, rank or position with an organisation listed in the order. See section 4.6-4.10 of the **CHIS Code of Practice, 2018**.

8.4. International deployments

Operatives from UK law enforcement agencies may be authorised under the RIPA for international deployments.

See section 4.6-4.10 of the **CHIS Code of Practice, 2018**.

8.5. AO and authorisations

AOs (see 3.7 for role specifics) should, where possible, be independent of the investigation. It is, however, recognised that this is not always possible, especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons.

They must be of the appropriate rank (or grade equivalent) and have completed accredited training. See annex B of the **CHIS Code of Practice, 2018** for a table of authorisation levels.

All undercover authorisations (foundation, advanced or UCOL) require authorisation at assistant chief constable rank or equivalent to the first cumulative total of 12 months. **Please note: urgent, long-term authorisations and likely access to confidential information are described below.**

The IPCO must be notified of all authorisations within seven working days.

8.5.1. Urgent oral authorisations

In urgent cases where it may not be practical for the application to be considered for oral authorisation by an assistant chief constable or equivalent, urgent authorisation may be given in writing by a RIPA AO-trained superintendent or equivalent.

Urgent oral and urgent written authorisations last for no more than 72 hours, at the conclusion of which a cancellation or renewal must have been submitted, as appropriate.

8.5.2. Long-term authorisations and confidential information

The AO must be at chief constable rank or equivalent, where one of the following applies:

- an existing authorisation will, or is believed likely to, exceed 12 months (long term, see **Statutory Instrument 2013/2788**)
- an authorisation is intended, or likely, to acquire confidential information – (confidential information includes legally privileged material, confidential personal information, confidential constituent information and acquiring confidential journalistic material and journalist sources). See **chapter 8 of the CHIS Code of Practice**, 2018) for further information. **In this case, the relevant period of authorisation is three months.**

The IPCO Judicial Commissioner must give prior approval, and the authorisation comes into effect once this is acknowledged by the AO.

Authorisation periods

Authorisations for relevant sources may be granted for an initial period of 12 months unless the same relevant source is already involved on the same investigation or operation.

The 2013 Relevant Sources Order defines long-term authorisation by reference to the cumulative periods for which the relevant source will be/has been authorised on the same investigation or operation (**5.27 CHIS Code of Practice, 2018**).

A long-term authorisation is one where the cumulative periods exceed 12 months, or, where the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 ("the 2010 Legal Privilege Order") applies, three months. If a relevant source has not been authorised on the same investigation or operation for at least three years, any previous authorisations will be disregarded for the purposes of calculating the 12 months.

When deciding if the relevant source is authorised as part of the 'same investigation or operation' in calculating the period of total or accrued deployment or cumulative authorisation periods (**5.28 CHIS Code of Practice, 2018**), the following should be considered:

- common subject or subjects of the investigation or operation
- the nature and details of relationships established in previous or corresponding relevant investigations or operations
- whether or not the current investigation is a development of or recommencement to previous periods of authorisation, which may include a focus on the same crime group or individuals
- previous activity by the relevant source that has a bearing by way of subject, locality, environment or other consistent factors should be considered in calculating the period
- the career history of the 'relevant source'

See examples in **5.30 of the CHIS Code of Practice, 2018**.

8.5.3. Nine months

Where an authorisation will, or is believed likely to, exceed 12 months, a notification form must be sent to the IPCO at the nine-month point. Where a UCO is deployed beyond the nine-month stage but a renewal will not be sought at 12 months, the IPCO should be informed.

Following receipt of the nine-month notification form, an IPCO inspector will be identified to undertake a detailed inspection of all necessary authorisation records.

The IPCO inspector will produce a report for the Judicial Commissioner in advance of the formal renewal request from the law enforcement agency. This report will subsequently be sent from the IPCO to the AO in the relevant law enforcement agency who is responsible for considering the renewal.

8.5.4. Eleven months

The AO (chief constable) should consider the renewal at the 11-month stage. This is to allow sufficient time for the IPCO Judicial Commissioner to consider whether to authorise prior approval.

8.6. Reviews

Regular reviews, as determined by the AO, are required to update the AO on any change in circumstances, impact on the necessity, proportionality, collateral intrusion and associated risk of the activity and UCO security and welfare.

The requirement for reviews is set out in sections 3.13 to 3.17 and in sections 8.9 to 8.11 of the **CHIS Code of Practice, 2018**.

If there is a likelihood for additional UCOs to be deployed on the operation, this must have been reflected in the initial application for the AO to consider this at the review stage. See **sections 93-99 of the OSC** procedures and guidance 2016.

8.6.1. Review documents

Review documents are made up of:

- the authorisation
- a review document
- an updated risk assessment, if appropriate

8.7. Renewals

All renewals other than following urgent oral authorisation require authorisation at chief constable rank or equivalent, with prior IPCO Judicial Commissioner approval (see **Statutory Instrument 2013/2788**).

8.7.1. Renewal documents

Renewal documents should include:

- an application for the renewal
- a risk assessment for each operative to be deployed
- once a decision has been reached, the authorisation or refusal
- details of the oral application and authorisation, where appropriate
- IPCO inspection report after review of the documentation associated with the undercover deployment

Also include:

- any appropriate IPCO comments
- advice from the prosecutor, if appropriate
- a letter of request, if appropriate (overseas)

If a law enforcement agency has not requested the renewal authorisation of a specific UCO within the requisite timescales they must cancel that UCO's use and conduct at the end of the authorisation period, and immediately seek a new authorisation.

During the intervening period, the UCO should not be deployed. Where circumstances demand that they have contact with subjects (for reasons of safety or to deal with a situation involving risk to life or the serious jeopardy of the operation), the AO should consider whether an emergency authorisation lasting 72 hours should be granted. IPCO must be informed at the earliest opportunity and advised of the remedial action taken. (See **paragraph 54 of the OSC guidance**).

8.8. Cancellations

There are two stages to the cancellation process:

1. cancellation by the AO
2. notifying the IPCO

An application for cancellation and the personal risk assessment, where appropriate, must be presented to the AO.

For any UCO activity that was likely to obtain confidential information, the IPCO Judicial Commissioner must be informed whether such material or information has been obtained and, if so, what steps have been taken to manage the material.

8.8.1. Cancellation documents

Cancellation documents are made up of:

- an application to cancel
- an authorisation to cancel
- a risk assessment, if appropriate
- an IPCO cancellation notification form

9. Planning, risk and deployment

Undercover units will deliver the undercover tactic on behalf of investigation/operational teams. The undercover unit is central to the planning, risk management and deployment of UCOs.

Contents

9.1. Planning

Teams wishing to deploy undercover tactics should liaise with the undercover unit whenever an undercover deployment is being considered. This assists operational/intelligence owners to consider the potential options available for covert tactics and methods.

Undercover unit staff will have a discussion with the operational team to clarify the operational objectives to explore the most appropriate tactics to meet those objectives. See 3 Infrastructure.

As undercover deployments are principally to gather evidence, early consultations with prosecutors must form part of the overall strategy and planning process between the COM-UC and the operational lead.

All requests for deployment of undercover resources must be supported by the relevant law enforcement agency tasking regime with senior management governance.

The operational lead must maintain a sensitive policy/decision log in all areas relating to the undercover tactics.

9.1.1. Initial planning

Initial planning should involve contacting the relevant undercover unit(s) where appropriate. It is the responsibility of the COM-UC to do this. This is to understand any particular sensitivities in the local community where a UCO is to be deployed and be aware of similar activities being undertaken by other public authorities which could affect the deployment.

Contact should always be made in advance with the undercover unit in the Police Service of Northern Ireland when planning to operate in Northern Ireland, and Police Scotland when planning to operate in Scotland.

Initial planning must consider the possible need for increased resources over time. The operational lead and undercover unit need to show that they have considered resource implications beyond initial deployment.

The undercover unit must be able to provide sufficient personnel and equipment to safely achieve the objective(s) of the deployment. The operational team must

maintain the provision of the investigative support throughout the life of the deployment. This operational support is to be agreed at the outset.

All decisions made in respect of undercover activity should adhere to **national decision model** principles and comply with NUWG standard operating procedures.

9.1.2. Assessing options

The operational lead will record the rationale for why the UCO tactic has been selected, what other tactics were considered and why they have been discounted.

9.1.3. Making decisions

The decision as to which tactic(s) are most appropriate to deploy to achieve the desired operational outcome should be made by the undercover unit in consultation with the operational lead.

If there is a conflict between the operational lead and the undercover unit (for example, over specific tactics, UCO safety or media issues), the head of the undercover unit should refer the matter to the person with overall responsibility for the undercover discipline in the force or agency.

9.2. Risk assessment

Risk assessments should be kept under constant review throughout deployments and proactively updated.

9.2.1. Operational risk assessment

Operational risks associated with proposed deployments should be addressed in the application for authorisation.

The operational lead, in conjunction with the COM-UC, is responsible for ensuring that the operational risk assessment is completed and maintained throughout the operation. The operational lead must provide information to assist the COM-UC in revising and maintaining ongoing risk assessments. This responsibility is throughout the duration of the investigation.

9.2.2. UCO risk assessment

A risk assessment must be completed for each UCO deployed.

The COM-UC, in conjunction with the cover officer, is responsible for ensuring that risk assessments are completed and reviewed throughout the operation.

The COM-UC must ensure UCOs are made aware of additional health and safety and control measures covering generic issues such as:

- safe handling of firearms
- arrest procedures
- needle stick injuries

(Note: this list is not exhaustive).

9.3. Pre-deployment responsibilities

Prior to deployment, the operational lead and cover officer must ensure that all UCOs have the following instructions read to them.

- UCOs must not act as an ‘agent provocateur’. This means they must not incite, instigate or procure a person, nor through that person anybody else, to commit an offence, or an offence of a more serious character, which that person would not otherwise have committed.
- UCOs may engage in an offence that is already laid on and may express interest and enthusiasm for proposals made even though they are unlawful.
- UCOs should behave in a manner that is consistent and commensurate with the role they are performing. They should do no more than offer an unexceptional opportunity to a person, group or organisation to commit crime. In doing this, they may demonstrate a degree of persistence and active behaviour where this is necessary to achieve the objectives of the investigation, if they do not coerce, instigate or incite the commission of offences that would not otherwise have been committed.
- UCOs have an individual responsibility to ensure that their personal involvement in any operation in their undercover role has been specifically authorised. UCOs may be required to give evidence in court proceedings about their use and conduct and about any evidence they may obtain during their deployments.

The operational lead and cover officer must then ensure the UCO:

- acknowledges receiving instructions by signing a copy (the supervising officer should sign the instruction document with inclusion of the date and time of the signature). The operative should add the name of the supervising officer who read the instructions, and sign the document using their pseudonym to confirm that the instructions were read to them, using the following wording:

  > 'These instructions were read to me prior to my deployment on this investigation/operation. I consent to the recording of any telephone conversations or other electronic communications, which I am "party" to in respect of this operation'.

- views the specific details of their authorisation for use and conduct
- is briefed on the objectives/tasks of their deployment

The COM-UC must ensure a governance system is in place to make sure that UCOs are regularly read the instructions throughout the operation. Once a deployment has begun, the cover officer should make sure requirements are adhered to and documented. See 3 Infrastructure.

9.3.1. Substance misuse testing

Every member of a law enforcement agency is subject to their force or agency's substance misuse testing policy.

9.4. Deployment responsibilities

9.4.1. Briefings and debriefings

At the planning stage of the undercover operation, the COM-UC and operational lead will agree the briefing and debriefing strategy. This will include those required to attend.

The cover officer must attend every operational briefing and debriefing. This is so that they can:

- manage UCO welfare and security
- make certain that evidence, intelligence and information is recorded correctly
- advise the operational lead and the operational team about tactical options

See also **APP on briefing and debriefing**.

9.4.2. Working hours

Those involved in undercover deployments must consider the **Working Time Regulations 1998**. They remain subject to legislation and the regulations and rules governing the respective law enforcement agencies' rules and regulations regarding working hours.

The cover officer and UCO should make sure they are not mentally or physically fatigued while deployed on operations. The COM-UC will regularly review the hours worked and the effect this is having on the UCO, the cover officer and the operation.

UCOs and the cover officer must inform the COM-UC or operational lead if they are suffering from mental or physical fatigue. The COM-UC must make sure UCO and cover officer working hours are recorded accurately.

9.5. Post-deployment responsibilities

The need to protect UCOs continues after cancellation of the use and conduct authorisations (see sections 5.29 and 6.13 of the **CHIS Code of Practice, 2018**). Any material which could compromise the identity of UCOs or covert tactics should not be disclosed without prior agreement from the COM-UC.

It is a shared ongoing responsibility between the undercover unit and the operational lead to ensure all efforts are maintained to recover and protect any material which could identify UCOs or covert tactics.

9.5.1. Compromise and exposure

The cover officer must report any exposure or compromise of covert methods and tactics.

Any subsequent reports that refer to the UCO (for example, commendations) should be compiled only in consultation with the undercover unit. Any commendations should not make reference to undercover activity.

9.5.2. Preparation of evidence

UCOs' statements must be typed to protect the identity of the UCO.

A system agreed by the COM-UC must be established for compiling transcripts for subsequent checking by the relevant UCO.

UCOs from foreign law enforcement agencies may compile their original notes and statements of evidence in English or in the language with which they are most familiar.

9.6. Use of technical equipment

When consideration is given to deploying UCOs together with technical equipment, the risk to UCOs should be balanced against operational requirements. The operational team should consider independent corroboration by other means, regardless of whether UCOs are deployed with technical equipment.

The COM-UC, in consultation with the cover officer, will agree a policy for the use of technical equipment and management of any product. This policy, together with any deviation, must be documented in the relevant policy/decision log.

The operational lead must document the security and handling procedure of any product in their sensitive policy/decision log.

An NUWG sub-group evaluates technical equipment for suitability and security.

The COM-UC may decide to use equipment additional to or other than that evaluated by the NUWG. This will be documented in the sensitive policy/decision log.

10. Witness anonymity

It is the responsibility of all law enforcement agencies to protect the identity of UCOs. This is an ongoing requirement, and extends beyond the period of the operative's undercover tenure. Following training, UCOs always deploy under a pseudonym to minimise the risk of exposing their true identity.

Contents

10.1. Witness anonymity orders

The COM-UC and cover officer should make sure there is early consultation with the prosecutor about all requests for witness anonymity orders. The discussions in relation to anonymity will take place during the earliest consultation with the CPS, and well in advance of any UCO being required to give evidence.

The court may provide a witness anonymity order when it is satisfied that the conditions outlined in **section 88** of the Coroners and Justice Act 2009 are met. See **section 89** of the Act for relevant considerations.

To comply with condition B in section 88 and with section 89, anything relevant to the UCO's credibility as a witness must be made known to the prosecutor. In all cases form MG6B (police misconduct material) or equivalent must be submitted to the prosecutor for each UCO in respect of whom an order is sought.

Before an application for a witness anonymity order can be made, the COM-UC should make sure a superintendent's (or equivalent) letter of authority and an associated risk assessment are prepared and submitted to the prosecutor.

See also **sections 86 to 90** of the Act, which provide more detail about the witness anonymity process.

10.2. Letter of request for UCO anonymity

The letter of request for UCO anonymity sets out the protection measures that are required. This request is completed by the superintendent (or equivalent) who has oversight and responsibility for the undercover unit.

It is also good practice to seek permission for the UCO to be permitted to enter, remain and leave the court in a way that does not reveal their identity.

10.3. Risk assessment

The risk assessment(s) must consider the risk factors for each UCO, and individual circumstances of the operation. It is not appropriate to submit a template risk assessment that fails to consider the factors specific to each individual.

Where specific risks to UCOs are identified, the risk assessment document will be retained by the relevant undercover unit and made available for consideration by the

prosecutor. It is the responsibility of the COM-UC to manage the creation, movement and retention of these documents. Revelation and disclosure of any of these documents must also be overseen by the COM-UC.

10.4. Hearing of the application

The hearing of the application will be conducted in the presence of the defence. If the prosecutor needs to refer to any sensitive material for the application, the defence will be excluded from this part of the hearing.

UCOs will not compile a statement in their true identity or National Index Number. The statement should only be completed in pseudonym, preferably in the first name.

The superintendent or equivalent or their nominated representative (usually the COM-UC) will attend court, if required, when the application is made with the original documents relied on in support of the application.

10.5. Giving evidence

UCOs will give evidence under their pseudonym. If required to do so, UCOs will reveal their true identity to the judge. This is usually done by discreetly offering their official identification (for example, warrant card) to the judge alone. The NUWG must be consulted should there be any variation to this process.

The COM-UC is responsible for ensuring:

- there are arrangements to safely transport UCOs and maintain their security during court proceedings
- liaise with the investigation team and court to manage media interest in the evidential process (see paragraph 6.5 for further information on media strategy)
- the measures outlined in the witness anonymity order are complied with

The COM-UC can request a change of venue via the CPS where sufficient security is not available, or other circumstances exist which are deemed inappropriate.

Nothing should be documented or communicated to the court that could identify UCOs or their force or agency.

11. Records

All records associated with undercover deployments and UCOs should be kept and maintained securely.

Contents

11.1. Record keeping

In addition to retention requirements under the **Criminal Procedure and Investigations Act 1996** (CPIA), all records must be kept available for inspection by the IPCO.

The head of unit will ensure all appropriate records are maintained securely.

The following points should be considered:

- information and intelligence should be evaluated and disseminated in accordance with the principles of **information management**
- records are subject to continual review in accordance with information management processes
- any electronic system should ensure an audit is maintained of all comments and amendments

11.2. Sensitive policy/decision log

The operational lead and COM-UC should consider including the following when completing a sensitive policy/decision log:

- operational objectives
- staffing
- security
- RIPA
- risk assessments
- psychological assessment reports
- briefings and debriefings
- intelligence management
- technical
- forensic strategy
- exhibits and disclosure
- prosecutor
- media strategy

11.3. Deployment records

Records must be maintained by the cover officer for:

- briefing and debriefing of the UCOs
- objectives set
- operative tasking
- reading of UCO instructions
- safety parameters

The frequency of the briefing and debriefing process should be commensurate with the nature of the deployment.

11.4. UCO original notes

UCOs should keep comprehensive records of events to an evidential standard. The undercover unit should provide UCOs with a means of recording evidence when operationally deployed (for example, an electronic or pocket notebook). The UCO must make their notes at the first available opportunity post-deployment. If they do not do this, they should give the reason for the delay in the original notes. The notes must be completed by the UCO prior to the commencement of the debrief. Where circumstances exist requiring immediate action (ie, prior to notes being completed), the reason for this must be noted by the UCO and the cover officer. These original notes should be presented regularly to the operational lead/COM-UC for review.

The COM-UC must ensure a log is maintained of the issue and return of all UCOs' original hard copy notes. There must also be a governance process in place to manage all electronic notes.

UCOs should record notes regarding each deployment in the respective record at the earliest opportunity. The cover officer should also make a policy entry for protracted delays due to extended deployments.

11.4.1. Format and content

UCO original notes should be completed in pseudonym. Original notes/books should also have unique reference numbers.

When completing an entry in their original notes, UCOs should observe the 'ELBOWS' mnemonic (see below), as appropriate, depending on whether it is electronic or hard copy. They should include the following information:

- the time the notes started and concluded
- a detailed sequence of events
- details of exhibits, including continuity
- details of any material or conversations used to refresh their memory

ELBOWS mnemonic

no **E**rasures

no **L**eaves torn out

no **B**lank spaces

no **O**verwriting

no **W**riting between the lines

Statements in direct speech

11.4.2. Recordings

A note should be made to say that a recording was made, but the original notes should not identify the type of equipment or recording methods used. These details are kept in a separate record. An audit of the booking in and out of equipment should be maintained by the cover officer. Any failure of the equipment will be documented by the cover officer.

Where there has been a recording, the conversation can be paraphrased.

Where there has been no recording, a full entry of the conversation will be made.

11.5. Material that might identify a UCO

The COM-UC should liaise with the operational lead to make sure any material that might inadvertently identify a UCO is gathered, reviewed and secured.

Such material could include:

- UCO original notes
- audio/visual products

11.5.1. Operational team

In consultation with the COM-UC, specified members of the operational team will have access to original notes and associated product generated from the deployment. This will be at the direction of the COM-UC who will consider access on a case-by-case basis. Sensitive material which could place the UCO at risk should not be handed over to the operational team.

Anything that could identify UCOs should be redacted before access is given. This may include redacting handwritten notes and images and audio of UCOs.

When a PACE interview is being recorded, interviewing officers should make sure no part of any recorded material featuring UCOs is played to a suspect so as to avoid exposing the identity of the UCO (eg, image, voice).

The defence must not be provided any access to sensitive material without agreement of the COM-UC.

11.5.2. Prosecution team

As is the case for all investigations, the prosecutor must be made aware of all relevant material in line with the CPIA, including material that assists the case for the accused.

In consultation with the head of unit, the reviewing lawyer will be granted supervised access to original material.

Copies of redacted (non-technical) material may be given to the prosecution team. All material provided must be stored securely.

11.5.3. Defendant and defence team

In consultation with the prosecutor or by direction of the court, the defence team may be granted controlled access to material with appropriate safeguards. Safety measures may include redaction, pixelation and sanitisation.

When providing controlled access to material, adequate facilities should be made available so that defendants and their legal representatives can listen to or view recordings (R v DPP and another, ex parte J. and another [2000] 1 WLR 1215). The COM-UC will put measures in place to ensure the defence cannot copy or record the material.

Where defendants have been remanded in custody, recordings and recording equipment may need to be taken to the prison or remand centre. The defence may challenge these arrangements and seek a direction from the court that they are provided with copies. The operational lead in consultation with the COM-UC should liaise with the prosecutor to make sure all proper arguments are advanced when resisting such defence applications.

Unless ordered by a court, no video or audio product, image or other item that could identify a UCO or expose covert methodology or sensitive tactics, may be served on the defence. In this event, consultation with the NUWG must take place before any material is shared.

About the College

We're the professional body for the police service in England and Wales.

Working together with everyone in policing, we share the skills and knowledge officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help those in policing develop the expertise needed to meet the demands of today and prepare for the challenges of the future.

college.police.uk