Corporate Policy

SERVICE INSTRUCTION

SI Identification Number	SI0116
Policy Ownership	Crime Operations
Issue Date	19/01/2017
Review Date	5 years from issue date
Last Updated	26/07/2021
Governing Service Policy	Intelligence Management
Cancellation of	SP2/2013 Handling of Confidential Information Supplied by Members of the Public
Classification	**OFFICIAL [PUBLIC]**

SI0116

Confidential Information from Members of the Public

This Service Instruction seeks to provide instruction on how The Police Service of Northern Ireland (PSNI) manages information provided by members of the public and increase public confidence in how information is handled.

Keeping People Safe

Table of Contents

Table of Appendices

1. Introduction

Police officers have a duty to obtain information and to handle it in an appropriate manner. At the outset, clarification should be sought from the member of the public providing information as to their willingness to provide such information evidentially. If this is the case there is no need to record this information as intelligence, instead a statement of evidence should be recorded.

This instruction relates to information obtained from the public by police officers or police staff where there is an expectation, that it will be treated in a confidential manner.

The need for confidentiality can arise because the individual faces personal, professional or other risks by passing the information to the Police.

The expectation of confidentiality is not absolute.

The necessity for the police to act on information received may override the need to protect the confidentiality of that particular individual.

2. Process

Members of the Public

A member of the public (MOP) is any individual who contacts the Police Service with information and expects it to be handled in a confidential manner. This also applies to individuals who contact the Police Service with information as part of their vocation or employment such as social workers, teachers etc.

Responsibilities

Any police officer or member of police staff who receives information from a MOP should create an intelligence submission on Police Systems prior to the termination of duty.

Police officers or members of police staff, who receive information from MOPs while not on duty, should create the intelligence submission as soon as practicable except in cases of Threats to Life or Crime in Action. In such cases the officer or member of staff must arrange for the information to be submitted as soon as possible.

Members of police staff who do not have access to Police Systems, but receive information from a MOP should immediately inform a colleague who does

have the relevant access and can complete a submission on their behalf. The original receiving member's staff or service number must be recorded where required.

It is the duty of all officers and police staff receiving information from MOPs to provide, to the best of their ability, the provenance of such information, including the identity of the MOP.

All original notes created by police officers or members of police staff when in receipt of information from a MOP should be retained by that officer or member of staff in accordance with the current retention of documents policy and the Criminal Proceedings and Investigation Act 1996.

Under no circumstances should the identity of a MOP be recorded on any paper-based system along with information that has been passed to police.

There are inherent risks involved in passing information to the Police Service. The identity of MOPs must remain confidential. Investigators who receive intelligence from a MOP and feel that they require further information or context, should request this from C3 Intelligence Branch.

If investigators believe that the MOP providing intelligence is a suspect in a criminal investigation, this should be communicated to C3 Intelligence Branch. The decision to divulge any further information regarding the source of the intelligence lies with the Head of Intelligence.

It is the responsibility of police officers and staff who receive MOP information to request that it be provided as evidence by way of a witness statement. Such statements should be recorded by a relevant officer.

All information provided by MOPs will be subject to current intelligence grading system. C3 Intelligence Branch will assess the information with other available information and come to a balanced assessment of the grading.

Threats to Life and Crime in Action

Any police officer or member of police staff receiving first notification of a threat to life or crime in action will obtain all the available information and then refer the matter to a Line Manager as soon as practicable, unless it is known to the officer that the information relates to a real and immediate threat, in which case it must be

referred to the officer's Line Manager with immediate effect.

Line Manager's in receipt of threats to life, whether real or potential, should refer to and comply with directions set out in the Threats to Life Service Instruction.

Any police officer or member of police staff receiving information from a MOP relating to Crime in Action should ensure that the information is disseminated to C3 Intelligence Branch verbally with immediate effect or the duty Inspector if outside office hours.

This process must always be followed by an intelligence submission on Niche via the PSNI Portal which will include a record of all action taken.

3. Juveniles and Vulnerable Persons

There are obvious risks involved in receiving information from juveniles and vulnerable persons. This should not preclude such information from being processed and being acted upon by police if appropriate.

Great care should be taken when dealing with juveniles and vulnerable adults and a specific risk assessment should be compiled in these circumstances. Such cases must be referred to the C3 Intelligence Branch. Consideration may be given to the involvement of a responsible person or appropriate adult.

All recommendations and decisions will be recorded in the electronic policy log attached to the MOPs nominal on Police Systems.

Any planned contact with a juvenile or vulnerable person, should be authorised by an officer of inspecting rank. These details will be recorded in the relevant policy log.

4. Intelligence Nuisance

Where C3 Intelligence Branch assesses that an individual has supplied information which is false or assessed to be purposely misleading, the matter will be referred to the C3 Intelligence Superintendent who has the discretion to have the MOP recorded as an 'Intelligence Nuisance' and flagged as such on Police Systems.

5. Reviews

It is essential that a MOP's status and any information they provide is reviewed. The need for this review will be identified by C3 Intelligence Branch and the review carried out by a C3 Intelligence Superintendent.

Where a MOP is in contact with the police on a repeated basis, the relationship between the MOP and the police and the information they have passed must be subject of review.

A review will be conducted after a maximum of every three contacts with police. C3 Intelligence Branch has discretion to identify an early review at any time should circumstances dictate. These circumstances include instances where a MOP provides information on terrorism or serious crime.

The purpose of a review is to:

- Ensure that no unregulated activity is taking place i.e. information is not being gathered in contravention of the Regulation of Investigatory Powers Act 2000 (RIPA) and therefore "status drift" has not occurred;
- Recognise and suitably mitigate any risks associated with the MOP or information they have provided; and
- Identify MOPs for referral as potential Covert Human Intelligence Source (CHIS).

All reviews, recommendations and associated decisions will be recorded in the electronic policy log attached to the MOP's nominal on Police Systems. It is the responsibility of the officer or staff making the decisions and recommendations to record them.

6. Status Drift

The term 'status drift' defines a situation whereby a MOP meets the definition of a CHIS

A CHIS is defined under Section 26(8) RIPA 2000 as 'a person is a CHIS if they:

- Establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the points below;

- Covertly use such a relationship to obtain information or to provide access to any information to another person; or

- Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

It is the responsibility of all parties involved in the submission and management of MOP information to monitor the relationship with the MOP and ensure that this situation does not arise.

In such instances it is for the C3 Intelligence Branch to determine if the officer or member of staff is managing the MOP as a CHIS or whether the MOP should be referred to a CHIS management unit within C3 Intelligence Branch.

Should it be assessed that the MOP is currently being managed as a CHIS, the assessing officer should take immediate action to ensure that this practice ceases forthwith and that the case is referred to a suitable C3 Unit.

Failure to comply may lead to a breach of RIPA and possibly to Discipline and/or Criminal Proceedings.

7. Risks

The PSNI Head of Intelligence (HOI) is the designated risk owner for all risks associated with the management of MOPs.

It is the duty of all officers or police staff receiving information from MOPs to highlight any identified or perceived risks associated with this information immediately to C3 Intelligence Branch. This information should also be recorded in the appropriate part of the Intelligence Submission Form at the time of submission.

Risks, once identified, should be highlighted in the MOPs Policy Log on Police systems. The generic risk assessment should then be consulted. The Generic Risk Assessment is included at Appendix A.

Any foreseeable risk not included should be subject of a specific risk assessment. This specific risk assessment template will be completed by the officer submitting the information from the MOP. The specific risk assessment template is included at Appendix B.

Where police officers or police staff are involved in receiving information from a

MOP they should, where possible, meet the MOP face-to-face in a safe environment. Under no circumstances should officers or staff who are not trained or authorised in covert techniques attempt to employ such techniques when meeting with a MOP. Such practices could not only lead to a compromise of the MOP but also a risk to officer safety.

There are substantial risks involved when receiving information from a MOP via text message. The possibility exists that the MOPs phone may be compromised but also the provenance of the information cannot be determined. This practice is to be actively avoided and the MOP advised accordingly.

If information is received in this way contact with the relevant MOP should be sought prior to any subsequent action. In any case a suitable assessment should be completed by C3 Intelligence Branch.

Appendix A Generic Risk Assessments

GENERIC RISK ASSESSMENT

Risk Type	LEGAL
	RISK ASSESSMENT
Risk Identified	There is a risk that during a criminal trial disclosure process, details of MOP information may be disclosed to the prosecution.
Probability	Low
Areas of Impact: ***Reputation*** ***Operational*** ***Person*** ***Economic***	 High Medium Low Medium
Overall Impact	Medium
Evidence	Information received from MOPs needs to be effectively managed under the Criminal Procedures and Investigation Act 1996. Failure to do so can lead to the unnecessary disclosure of confidential information and possible compromise of the MOP.
	RISK MANAGEMENT
Control Measures	• All MOPs managed in accordance with PSNI procedures. • Information will be processed in accordance with PSNI procedures and National Guidance. • Sensitive Disclosure Unit will be consulted at an early opportunity should judicial proceedings appear likely. • Sensitive Disclosure Unit will seek to ensure MOP identities are protected in the context of any criminal trial proceedings.

GENERIC RISK ASSESSMENT

Risk Type	LEGAL
	RISK ASSESSMENT
Risk Identified	There is a risk that if information received from a MOP is not managed properly then PSNI will fail in its legislative obligations.
Probability	Low
Areas of Impact: ***Reputation*** ***Operational*** ***Person*** ***Economic***	 High Medium Low Medium
Overall Impact	Medium
Evidence	Information received from MOPs needs to be effectively managed. Failure to do so can create situations where justice is not served, with offenders not being brought to justice or a failure to prevent crime.
	RISK MANAGEMENT
Control Measures	• All MOPs managed in accordance with PSNI procedures. • Information will be processed in accordance with PSNI procedures and National Guidance.

GENERIC RISK ASSESSMENT

Risk Type	PHYSICAL
	RISK ASSESSMENT
Risk Identified	There is a risk that if poor methodology is used in meeting or contact with the MOP the MOP will be compromised.
Probability	Medium
Areas of Impact: **Reputation** **Operational** **Personal** **Economic**	 High High Very High High
Overall Impact	High
Evidence	The nature of the history in Northern Ireland and the small geographical size of the country means that there is a danger that the MOP may be compromised when in contact with the police. It must be borne in mind that if a MOP is compromised they may well be physically assaulted or they may have to be placed in a protected persons scheme at considerable expense.
	RISK MANAGEMENT
Control Measures	• If MOPs are being physically met, they should be met within a safe environment and these locations should be rotated to limit the chances of compromise. • All MOPs will be subjected to review. • Information from a MOP via mobile phone text message should not be actioned without a subsequent corroborative contact or assessment by the C3 District Intelligence Unit.

GENERIC RISK ASSESSMENT

Risk Type	PHYSICAL
	RISK ASSESSMENT
Risk Identified	There is a risk that a MOP will self-compromise leading to them being physically attacked and/or threatened.
Probability	Low
Areas of Impact: **Reputation** **Operational** **Personal** **Economic**	 Low Low High Medium
Overall Impact	Medium
Evidence	MOPs may disclose the fact that they are passing information to the police to trusted family and/or associates. While this is not desirable for the most part it will not lead to the MOP being compromised to the wider community. However, a MOP may disclose their role to an inappropriate person or the relationship with their confidant may change leading to compromise.
	RISK MANAGEMENT
Control Measures	• All MOP cases are subject to reviews • MOPs will be instructed, where appropriate, to keep their relationship with the police confidential. • Where a MOP has self-disclosed, this information will be recorded on the MOP policy log.

GENERIC RISK ASSESSMENT

Risk Type	PUBLIC
	RISK ASSESSMENT
Risk Identified	There is a risk that if MOP information is not managed properly public confidence in the PSNI will be lost.
Probability	Medium
Areas of Impact: ***Reputation*** ***Operational*** ***Person*** ***Economic***	 High Medium n/a
Overall Impact	Medium
Evidence	Poor management of MOP information could lead to poor public perception of the PSNI. Such perception could cause considerable damage to community and PSNI relationships.
	RISK MANAGEMENT
Control Measures	• All MOPs managed in accordance with PSNI procedures. • Information will be processed in accordance with PSNI procedures and National Guidance. • All MOPs will be subject to review.

Appendix B Specific Risk Assessments

SPECIFIC RISK ASSESSMENT

Risk Type	
	RISK ASSESSMENT

Risk Identified	
Probability	
Areas of Impact:	
Reputation	High
Operational	Medium
Person	Low
Economic	Medium
Overall Impact	
Evidence	
	RISK MANAGEMENT
Control Measures	

Appendix C Contact Us

Service Instruction Author

D/Chief Inspector P18150

Branch Email

HQIH@psni.police.uk