



Management of Intelligence Policy (Surrey and Sussex)

Abstract

This policy articulates the principles by which Surrey Police and Sussex Police will discharge its functions in relation to the management of intelligence information which is crucial to providing a quality service to the public, partner agencies, other police forces and law enforcement agencies.

Supporting Documents

[Authorised Professional Practice \(APP\) guidelines](#)

[Data Protection Act \(2018\)](#)

[General Data Protection Regulation \(GDPR\)](#)

Policy

1. Introduction

1.1 This policy is required to ensure Surrey Police and Sussex Police (hereafter referred to as the Forces) comply with national legislation and [Authorised Professional Practice \(APP\) guidelines](#) with regard to the management of intelligence information. This is crucial to providing a quality service to the public, partner agencies, other police forces and law enforcement agencies.

Information is stored in a number of databases which represents a valuable asset to the Forces in the recording and management of intelligence. It is important that such information is retained so as to be accessible for operational policing and will:

- Give clarity and direction to police officers and police staff in the management of intelligence information and in the submission of intelligence.
- Improve the quality of electronic recording and management of intelligence information.
- Build confidence amongst police officers and police staff in the use of associated databases.

2. Scope

2.1 This policy covers the management and recording of intelligence information.

3. Policy Statement

3.1 Information is stored in a number of databases which represents a valuable asset to the Forces. Our primary database for Policing Information is NICHE and all criminal

intelligence of relevance to the Forces must be recorded on it in order that it is readily accessible for operational policing purposes.

The Forces will ensure that police officers and police staff who use and/or manage this information will be appropriately trained and have a good working knowledge of these systems in order to safeguard the information and to comply with the [Data Protection Act \(2018\)](#) and [General Data Protection Regulation \(GDPR\)](#).

Procedure

1. Introduction

1.1 All police officers and police staff using and/or managing Intelligence information systems will be appropriately trained and have a good working knowledge of the appropriate intelligence systems.

1.2 The Intelligence Report (IR) is used to submit and evaluate information, and to manage dissemination of intelligence. It protects the source and contributes to an audit trail of the intelligence. Standardisation of reporting provides a shared confidence between law enforcement communities and partner agencies. For more information on the Intelligence Report please refer to [APP](#)

1.3 The Forces use NICHE as the primary database for recording intelligence reports.

1.4 All police officers and police staff will be granted access to NICHE on successful completion of the pre-requisite training course applicable to their role.

2. Intelligence

2.1 All Intelligence must be recorded on NICHE within the following time frames:

- High priority - within 12 hours Monday – Friday, 18 hours Saturday-Sunday
- Medium priority – within 24 hours
- Low priority – within 72 hours

These time frames are initiated from when the intelligence is received by the Intelligence Processors in Force Intelligence Bureau (FIB) or Divisional Intelligence Hubs.

2.2 Individuals must submit intelligence immediately upon the first moment this is practicable.

2.3 The submission of any high graded Intelligence log must also be raised with the Individual's supervisor to ensure any immediate safeguarding responsibilities are carried out.

2.4 Officers or staff submitting intelligence are responsible for carrying out systems searches and basic research connected with the intelligence submitted in order to corroborate information given and provide context. For example if a vehicle index has

been provided, a Police National Computer (PNC) check would be expected; or if information is given relating to a crime then the crime reference or Operation name should be provided.

2.5 Specialist Crime Command (SCC) Intelligence Supervisors will assess actionable intelligence for risks and opportunities in accordance with control strategy priority areas. These will be taken to the Daily Management Meeting (DMM) as necessary. SCC Intelligence will also take intelligence to the DMM where prioritisation and resourcing decisions need to be made.

2.6 Officers or staff who are tasked with actionable intelligence are responsible for defining all subsequent actions relating to that intelligence, in support of intelligence development or investigative activity. This will be in line with Threat, Harm, Risk, Investigation, Vulnerability and Engagement (THRIVE) and reflect any prioritisation set at Tactical Tasking and Co-ordination Group (TTCG) or DMM.

2.7 Where information collected for any policing purpose, and recorded on other systems or held in hard copy form, impacts on the risk to the public posed by an offender then an intelligence record will be created in NICHE by the person receiving that information.

2.8 Information recorded for other policing purposes will be retained on the appropriate application, and for the necessary period, for that purpose.

2.9 Where policing information is recorded on other systems or held in hard copy form as a result of an investigation or operation then either during, or at its conclusion, the information held must be reviewed by the person responsible for that investigation or operation to assess whether any should be added into NICHE as an intelligence record.

2.10 It is the responsibility of staff engaged in partnership working for a policing purpose to collect any intelligence information identified from other agencies as a result of that working and ensure it is recorded on NICHE.