Information Management Policy (Surrey and Sussex) (1187/2025)

## Abstract

This document outlines information in relation to Information Assets, Sharing and Disclosure, Data Quality and Retention and Disposal of Information.

## Policy

### 1. Introduction

1.1 Information Management is the creation, collection, storage, curation, dissemination, archiving and destruction of information. Under the UK General Data Protection Regulation (GDPR), these activities are collectively referred to as data processing. This includes documents, images and other sources such as digital media (Closed Circuit Television (CCTV), Body Worn Video (BWV), etc). The Forces Information Management (IM) teams ensure that information held by the Forces complies with all relevant legislation and enables effective risk management.

### 2. Scope

2.1 This policy and procedure covers:

• Information Assets

• Sharing and Disclosure

• Data Quality

• Information Retention and Disposal

### 3. Policy Statement

3.1 The Forces recognise that managing information compliantly is the responsibility of all police officers, police staff, Special Constables, contractors and volunteers. All IM risks are reported to Senior Information Risk Owner (SIRO) at the Security and Information Management Board (SIMB) via the IM teams.

## Procedure

### 1. Information Assets

1.1 The Information Asset Register (IAR) lists the Forces Information Assets (IAs). IAs are managed by the respective Information Asset Owner (IAO) supported by an Information Asset Administrator. IAs are systems and practices which store or process personal information.

The IAR records the following information

• The business areas the IA is assigned to

• The Information Asset Owner (IAO)

• The Information Asset Administrator (IAA)

IAOs must inform the respective IM team of any changes to their assets, any incidents must be highlighted during the assurance process. Using this information, the IM teams assist and provide support regarding the planning and structuring of information held in assets.

1.2 It is the responsibility of the IAO for each asset to ensure that specific IAs owned by them are handled and managed appropriately, providing assurance and making sure any remedial action required is undertaken.

1.3 The IAO is responsible for handing over duties when they change roles. They must fully explain the expectations of the role to the new IAO and update Information Management to update the register. Further information on the IAO / IAA roles is detailed in the Information Asset Owner Policy (Surrey and Sussex) (1239).

**2. Sharing and Disclosure**

2.1 The key principles applied to the sharing, disclosure and dissemination of personal information (sharing of operational information / intelligence is managed under the National Intelligence Model) are:

• Where a legal gateway exists, this provides a specific purpose for sharing police information with an outside agency. Legal gateways may be under statutory obligation, statutory power or common law.

• Where a legal gateway is not readily identified, the decision to share is based on establishing a policing purpose and undertaking a risk assessment. Consideration should be made to the UK UK Data Protection Legislation (including the UK General Data Protection Regulation (GDPR)) and Article 8 of the Human Rights Act 1998 (right to respect for private and family life). It is often necessary to weigh the need for disclosure against the right of the data subject to privacy.

If this is regular sharing with the outside agency, it must be subject to an Information Sharing Agreement as described under section 2.3.

If in doubt obtain IM advice.

2.2 Sharing information must be succinct and as a minimum capture the below. It is advised that requests use the Data Protection form on the Force Intranet as this includes all the necessary data fields (Data Protection Request (DP2) Form):

• Full details of why the information is being requested and how it will be processed by the partner agency.

• The lawful authority / justification for sharing (example might be ‘safeguarding’ when sharing a risk assessment form or ‘prevention of crime’ when sharing with shop-watch).

• The date, time and identity of the person sharing.

2.3 Information Sharing Agreement (ISA)

Sharing with partner agencies who have a statutory power to share or receive information, where there is a frequent and continuing need for disclosure of information, require an ISA that clearly sets out standards and procedures should be used. Refer to Information Sharing Agreement Process and Information Sharing Agreements (ISA).

2.4 Where partners are Surrey agencies, it may be possible to utilise the existing Multi-Agency Information Sharing Protocol (MAISP) or the specific Crime and Disorder Information Sharing Protocol. Written agreements are not necessary when the sharing is between police services.

2.5 It is acceptable to share information outside of an ISA, provided the appropriate process is followed and a risk assessment undertaken. Please contact your Force Information Management team to see if an agreement exists.

2.6 All sharing of police information must be lawful and relevant, necessary and proportionate to achieve that specific outcome. See Section 2.2 for further information.

**3. Staff Name Disclosure**

3.1 The Forces will review applications to disclose the names of staff upon receiving a request, verbally or in writing, providing the person is:

• A police officer (regular or Special Constable)

• A senior police staff manager, defined as Band 1/ M1 Grade or above.

• A decision maker, defined as a member of staff who deals directly with the public, in person or in writing, or makes decisions on behalf of the Forces.

3.2 In line with the National Police Chief Council (NPCC) guidelines for Rights of Access requests (27.1.1), members of staff and officer names (below the rank of Band 1 / M1) will be exempt from disclosure requests. Members of staff and officers are considered data subjects for the purposes of the UK GDPR and as such, the above is a necessary process to ensure adherence to the data minimisation principles. As such, Forces have an obligation to protect their confidentiality and their right to privacy (Article 8 of the Human Rights Act 1998).

3.3 Staff name disclosure will apply in all circumstances except where the health or safety of the individual may be compromised. Such circumstances would include where officers are involved in Terrorist Operations. In these and other specific cases, a Health and Safety Risk Assessment will be completed. If there is any doubt about this, the decision to release a member of staff's name must be referred to their Divisional or Departmental Commander.

3.4 If a decision is taken not to release a member of staff's name in reply to a written request for information, the decision will be referred to the respective Force Information Access Team (IAT).

**4. Data Quality**

4.1 The Data Quality Team (DQT) (Surrey) and the Data Compliance Team (DCT) (Sussex) provide the Forces with confidence that the Niche database is being used correctly by users. The teams ensure the integrity of the data in order to maintain a highly effective, functional operational, tactical and strategic management tool that is compliant with all relevant legislation and guidance.

4.2 Data quality, although supported by the DQT / DCT, is the responsibility of the individual. Errors in Niche must be reported to the DQT / DCT as soon as possible for rectification. The teams are available to provide help and guidance to the user community to ensure accuracy of data.

4.3 Data quality in Police National Computer (PNC) and Police National Database (PND) is monitored by Disclosure Services (Surrey) / Force Research Bureau (Sussex). It is the responsibility of the user to notify their respective team if they notice any errors on these records.

4.4 It is essential that all records on police systems are accurate and up to date. It is every staff / officer's responsibility to ensure all details, including name and gender, are updated correctly. Misgendering is when someone refers to a trans person using the gender they were assigned at birth instead of their real gender. Referring to a transgender person by their birth name, even after they have transitioned or no longer use that name is called dead naming. When done deliberately this is deeply hurtful to trans people and can subject them to bullying and harassment. More details on updating gender can be found on the information hub.

4.5 It is the responsibility of all users and the Information Asset Owner for the Data Quality in data storage platforms used across Surrey Police and Sussex Police. These systems are not monitored by our DQT or DCT but they are available to provide advice around best practise in regards to Data Quality.

4.6 The Forces have Force Crime and Incident Registrars who monitor and ensure the correct recording of Crime on our core policing platform, Niche. Regular checks are carried out to ensure that crime is recorded correctly. The Force Crime and Incident Registrar and their deputies can provide advice when there is uncertainty.

**5. Retention / Disposal**

5.1 The Forces retention schedule is available by following th Surrey and Sussex Retention Schedule. There are slight deviations from the National Schedule. For changes or additional deviations to the retention schedule, contact the Management of Police Information (MoPI) team in Surrey.

5.2 The Forces recognise the importance of appropriate retention, storage and disposal of documents. Force records, evidence and property will be retained in a manner and for such time as is shown in the retention schedule.

5.3 The Force Evidential Property Manager and their team in Sussex, and the Information Governance Manager and their team in Surrey have authority to retain or dispose of records, evidence and property in accordance with legislation and national guidance.

5.4 The MoPI retention only applies to police information per se not to operational / corporate records falling outside the law enforcement criteria as defined at Section 31 DPA 2018. Ancillary records, evidence or property that do not contribute to understanding the nature of the offence, subject behaviour or type of risk imposed will be retained under other specific enactments or national guidance.

5.5 Any Electronic Document and Records Management System (EDRMS) operated within the Forces must have the relevant retention / disposal periods incorporated into the record type parameters. This applies to both physical and electronic records.

5.6 Documents and electronic media containing information classified as 'OFFICIAL' or above have specific disposal instructions. Individuals will be responsible for ensuring all police information is disposed of correctly refer to the Surrey Police and Sussex Police Information Security Policy (722).

**6. Supporting Documents**

6.1 Information Sharing Agreement Process

Risk Management Policy (Surrey and Sussex) (1049)

Data Protection Policy (Surrey and Sussex) (780)

Surrey Police and Sussex Police Information Security Policy (722)

Information Asset Owner Policy (Surrey and Sussex) (1239)

Rights of Access Policy (Surrey and Sussex) (1181)

Surrey only: Police National Computer (PNC) Procedure

Surrey only: Records and Evidence Centre Policy

Surrey only: Message Switch Police National Computer (PNC) Update Procedure

Surrey only: The Use of Police National Database (PND) Policy

Surrey only: Information Requests Procedure

Surrey only: Publication Scheme (Freedom of Information) Updating Procedure

Sussex only: Freedom of Information Policy (821)

Sussex only: Crime and Incident Disposal, Recording and Auditing Policy (757)

Sussex only: Police National Computer (PNC) Compliance Policy (900)

Sussex only: Use of the Police National Database (PND) Policy (1148)

**Team:** Information Management