# APPROPRIATE POLICY DOCUMENT FOR SPECIAL CATEGORY AND LAW ENFORCEMENT DATA

**We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.**

Owner: SIRO
Document ID: ICT-PL-0116
Version: 1.2
Date: March 2021
Review date: March 2023

## DOCUMENT MANAGEMENT

| Version | Date | Summary of Changes |
|---|---|---|
| 1.1 | December 2018 | First version |
| 1.2 | March 2021 | Review and Updates |
| 1.3 | September 2021 | Update |

| Accountable Owner | | Approval date |
|---|---|---|
| Senior Information Risk Owner (SIRO) | Chris Bally | 05/07/2021 |

| Responsible Owner | | Approval date |
|---|---|---|
| Head of Information Governance | Peter Knight | 21/04/2021 |

| Reviewers | Role | Approval date |
|---|---|---|
| **Policies Review Group**:<br>Russell Armstrong<br>Philip Barbrook<br>Anna Stephenson (policy review lead)<br>Joanne Withey<br><br>Corporate Information Governance Board - ratification | <br>IT Security Manager<br>Enterprise Architect<br>DPO & Compliance Manager<br>DP & Training Manager | 18/05/2021<br><br><br><br><br>29/07/2021 |

| Publication information | | |
|---|---|---|
| | **Published** (if YES, enter document location)? | **Location** |
| All staff | Yes | mySCC |
| Public | Yes | SCC website |

## Introduction

1. The UK GDPR and Data Protection Act 2018 (collectively referred to as data protection law) outlines the requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain conditions.

2. This policy sets out how the Council meets its obligations under data protection law and describes the compliance requirements for those responsible for processing special category (SC) and law enforcement (LE) data. The policy comprises:

   Part A: standard compliance requirements for processing SC and LE data, and
   Part B: additional compliance requirements for processing LE data.

3. This policy should be read in conjunction with the following policies:

   - Data Protection
   - Information Security
   - Security Incident Management and Reporting
   - Acceptable Use of Information Systems
   - Records Management

## PART A – PROCESSING SPECIAL CATEGORY AND LAW ENFORCEMENT DATA

1. SCC processes special category (SC) and law enforcement (LE) data. All SC and LE datasets should be recorded in each Directorate's Register of Datasets. Each dataset recorded in a Register includes both the lawful basis for processing and a further Data Protection Act 2018 Schedule 1 condition for processing SC and LE data.

2. The Dataset owners for SC and LE data are responsible for adherence to this policy and are accountable to the Council's Corporate Information Governance Board (CIGB) which includes representatives from each Directorate and/or its Services. SC and LE data issues can be tabled as an agenda item where required.

3. The Council's Senior Information Risk Owner (SIRO) can arbitrate where there are conflicts between business need and privacy/security matters. This will involve consultation with the Data Protection Officer.

4. All SCC workers must report information security incidents via IT Self Service *'Report an Incident'*. At the earliest stage it needs to be clear whether the data impacted by an incident is SC and/or LE personal data and 'sensitive processing' (i.e., special category data used for law enforcement purposes) as this will have a bearing on any notifications to the Information Commissioner.

5. Where appropriate SCC's Directorates and/or Services' specific privacy notices provide information about the processing of SC and LE data. Privacy notices are published on SCC's external website and Directorates and their Services should review them regularly.

6. To support SCC's technical and organisational measures which implement the data protection principles effectively and safeguard individuals' rights (this is known as 'data protection by design and by default'), Data Protection Impact Assessments (DPIAs) should be undertaken to assess the impact of using personal data for new purposes upon individuals' privacy. The DPIA template is available from the mySCC Information Governance pages. All DPIAs are reviewed and approved by the Data Protection Officer.

7. Individuals' rights under data protection law are detailed in SCC's corporate, Directorate and Service specific privacy notices. Individuals' requests to exercise their rights are managed through the corporate Information Governance team which keeps a record of all requests and their outcomes.

8. The Council has appropriate technical and organisational measures in place to protect the integrity and security of SC and LE data.

9. The following roles are responsible for ensuring compliance with this policy.

    a) **SIRO**: this role is fulfilled by the Deputy Chief Executive and Director of Corporate Services who is the accountable owner of this policy.

b) **Head of Information Governance** is the responsible owner of this policy and co-ordinates record-keeping activities with the Manager of the Records Management Centre.

c) **Managers** are responsible for ensuring that adequate induction and training is undertaken by all SCC workers and that support is provided to them where they are processing SC and LE personal data.

d) **Non-compliance with this policy** by staff could warrant further action and investigation under the Council's Disciplinary Procedures. In certain circumstances, non-compliance with this policy may be considered gross misconduct resulting in dismissal.

   Councillors found to be in breach of this policy may be non-compliant with the Members' Code of Conduct which may lead to a referral to the Council's Monitoring Officer.

## PART B – PROCESSING LAW ENFORCEMENT DATA

1. Part 3 of the Data Protection Act 2018 (DPA) deals specifically with the processing of personal data for criminal law enforcement purposes. There are specific requirements for this type of data processing.

2. For the most part the additional legislation in the DPA, relates to the work of 'competent authorities' (e.g., heads of police constabularies and other bodies listed in schedule 7). Although SCC is not listed as a 'competent authority' it does have statutory functions which relate to prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding of threats against public security.

3. SCC needs to ensure that it:

   a) Understands which relatively niche business areas/statutory functions the criminal law enforcement requirements apply to and is clear on legal purpose(s).

   b) Has a clear policy on how such personal data is processed and covering areas such as privacy by design, consent, transparency, and security controls such as auditing.

   c) The above is undertaken within the context of the overall UK GDPR framework (i.e., measures for the criminal law enforcement personal data **supplements rather than replaces** other parts of the UK's data protection law).

4. The following areas within SCC have been identified as Competent Authorities (see paragraph (2) above) and collect and process personal data specifically for law enforcement purposes:

   a) SCC's Trading Standards team who have statutory functions to detect, investigate and prosecute or execute fines etc.

   b) SCC teams who are tasked with investigating and prosecuting types of environmental crime and the execution of fines in connection with this work.

   c) SCC teams tasked with ensuring adherence to school attendance in accordance with statutory requirements. Council officials can take a decision to prosecute.

   d) SCC Youth Offending teams, who investigate and carry out proceedings in the criminal courts.

   e) Internal Audit & Counter Fraud Services, who from 2019 have approval to conduct criminal investigations (see Sanctions Policy on the SCC website).

5. Many parts of SCC hold information, including personal data, which could be subsequently used as evidence in criminal prosecutions, e.g., information held by social workers on case management systems relating to possible harm caused to a child/vulnerable adult or information held by internal audit relating to possible fraud.

   This information does **not**, however, constitute law enforcement personal data as defined by Part 3 of the DPA, instead this information will be processed under the General Processing Regime under Part 2 of the DPA. This is because SCC will not be the legal entity, which is investigating and prosecuting, i.e., the evidence will be passed on to the Police and the Prosecution Service who under data protection law, are defined as the 'competent authorities' to decide on any court action.

   Many parts of SCC may process personal data which is used in legal proceedings (e.g., care and protection orders or SCC seeking legal redress from a supplier), but these are undertaken within civil and family law courts/tribunals and are out of scope of Part 3 of the DPA.

6. Apart from the compliance risks (i.e., the consequences of not complying with all parts of the DPA including Part 3), which is the main driver for this policy, there are also security risks which relate specifically to the type of data within scope:

   a) The ability of SCC to carry out investigations and prepare prosecutions is severely impacted if the law enforcement personal data is viewed by non-intended persons (confidentiality), cannot be trusted due to it being corrupted or incomplete (integrity) or is not available when required by SCC officials.

   b) Public trust in the SCC teams tasked with action such as criminal prosecutions is severely impacted if the relevant personal data is not managed effectively with clear records management, access, storage and sharing procedures in place.

   c) The overall corporate reputation of SCC is impacted if it is not able to provide and share with partners, such as the Police, Courts and other agencies, the right data – including personal data – when necessary.

7. Where SCC processes personal data specifically for criminal law enforcement it will be in accordance with the Part 3 (DPA) data protection principles[1]:

   a) The processing of personal data for any of the law enforcement purposes must be lawful and fair. SCC will be clear upon which statutory law it is relying upon or whether it is appropriate to use consent. It will also only carry out sensitive personal data processing for law enforcement purposes where it can demonstrate that this is strictly necessary (as per schedule 8 of the DPA).

[1] These principles are very similar to the overall data protection principles set out in the GDPR.

b) The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit, legitimate and; personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

c) Personal data processed for any of the law enforcement purposes must be adequate, relevant, and not excessive in relation to the purpose for which it is processed.

d) Personal data processed for any of the law enforcement purposes must be accurate, and where necessary kept up to date and every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard for the law enforcement purpose for which it is processed, is erased, or rectified without delay.

f) Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

g) Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

8. Where any service or worker in SCC intends to process personal data for law enforcement purposes for the first time it must:

a) **Consult with the Data Protection Officer**: if the personal data in scope of the new processing is judged to fall within Part 3 of the DPA (and additionally if it is deemed to be 'sensitive processing'), then a data protection impact assessment (DPIA) must be undertaken prior to processing to ensure that the additional controls and safeguards required for this type of data are met.

b) **Identify the Dataset Owner**: the personal data that is to be processed within scope of law enforcement must be 'owned' by the appropriate senior SCC role and be listed in the Directorate's Register of Datasets (along with description of data, purpose (including statutory basis and a DPA schedule 7 condition)) and retention period.

c) **Privacy by design**: the Dataset owner must take steps to ensure that all appropriate measures are taken to safeguard the personal data within scope of law enforcement processing. In particular:

i. **Clear on legal purpose:** As per Principle 1 of the DPA to be clear on which legal basis[2] is being used.

ii. **Data segregation**: ensure that more general personal data processing is separate from that to be used for criminal law enforcement purposes as far as possible (e.g., dataset or database for investigations/proceedings not same as that for other customers of services).

iii. **Data minimisation & pseudonymisation**: Ensure that the personal data collected for the purposes of law enforcement is minimised in terms of:

a) only that personal data required for purpose (and 'special category'/sensitivity processing) when necessary;
b) minimal amounts stored and shared on a 'need to know basis'; and
c) pseudonymised where this is practical to do so (e.g., case management number when emailing).

iv. **Record keeping & logging:** data is retained as long as is necessary for business and statutory purposes and that there is an adequate audit logging functionality.

d) **Logging and auditing**

All SCC information systems have a form of audit trail. However, the bar for law enforcement personal data must follow a higher minimum standard to:

i. Be able to identify which person at SCC viewed or modified or erased the record.

ii. Be able to know the time/date that such access occurred.

iii. Be able to ascertain that the record is in scope of criminal law enforcement because of the structured record system in which it is held.

iv. Be able to records consent decisions from data subjects (if appropriate).

v. Be able to provide a comprehensive log on demand of access if required for internal audit or other purpose.

[2] Although it may not be appropriate to obtain consent from those persons who are subject of criminal investigations or proceedings, it will need to be considered whether consent is required for persons who are not the subject of the investigation but who provide personal data (e.g., witness statements) to aid law enforcement. If consent is required, then the means of recording this agreement (and explicit consent regarding sensitive processing of special category data) must be agreed prior to processing.

e) **Transparency**

SCC services which carry out personal data processing for law enforcement purposes must include due reference in their privacy notices of the purpose and nature of the processing (and the relevant statutory basis), the type of

data that is required and shared, how long it is retained for and the safeguards to ensure that this specific data is suitability separated from other types of non-law enforcement purposes.

Other background information shall be provided in SCC website content (e.g., Trading Standards Enforcement Policy) that makes clear how the criminal law enforcement aspects fit into wider functions where such personal data is collected for non-criminal enforcement purposes.

f) **Subject Access Rights**

SCC will take steps to ensure that where personal data is being processed for law enforcement purposes the subject rights will be met. Note: these rights differ from those in the UK GDPR (i.e., right to object and right to portability).