Scottish Courts and Tribunals Service

Law enforcement processing: Part 3 Appropriate Policy Document

Publication Date:	**27 May 2026**
Version:	1.5
Review Date:	Every two years

Scottish Courts and Tribunals Service

Version Control

Date	Version	Author Initials	Description of Change
September 2018	V1.1	IH	Created and published
24/10/2025	V1.2	LJ	Transferred to new policy template
06/02/2026	V1.3	LJ	APD split into two policies covering Law enforcement and general processing under UK GDPR. Full review and rewrite.
20/05/2026	V1.4	LJ/NA	Reviewed by Director of LIU
27/05/2026	V1.5	LJ	Published

Introduction

Part 3 of the Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing sensitive personal data for law enforcement purposes.

This policy explains the Scottish Courts and Tribunals Services (SCTS) procedures for securing compliance with the data protection principles listed below in relation to sensitive processing for law enforcement purposes.

It also explains the retention and erasure policies in relation to the sensitive processing. This policy is a requirement under section 42 of the Data Protection Act 2018 (the Act).

What is sensitive processing

Sensitive processing is defined in section 35(8), Part 3 of the Act and is equivalent to GDPR special category data. It includes:

> a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
> b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
> c) the processing of data concerning health;
> d) the processing of data concerning an individual's sex life or sexual orientation.

Law enforcement purposes

"Law enforcement purposes" is defined as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Subsections 35(4) and (5) of the Act state that sensitive processing for law enforcement purposes is permitted in only two cases, where the processing:

- is based on the consent of the data subject - section 35(4);

or

- is strictly necessary for the law enforcement purpose and is based on a Schedule 8 condition - section 35(5).

The purpose of this document is to demonstrate that the processing of this sensitive data by the SCTS is compliant with the requirements of section 42, Part 3 of the Act. Section 42(2) specifies that for the above processing, the APD should:

> (a) explain your procedures for securing compliance with the law enforcement data protection principles;
>
> (b) explain your policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

This document is a general policy for sensitive processing by SCTS. Where there are potentially high risks as a result of specific processing activities, a tailored policy document will be produced in respect of that activity, however, this will be on an exceptional basis.

Description of data processed

Schedule 7 of the Act provides that the SCTS is a “competent authority” for the purposes of Part 3 of the Act. We carry out sensitive processing for law enforcement purposes in three areas:

- Administration of justice;
- Fines enforcement;
- Archiving of criminal records under public records legislation.

We carry out sensitive processing in all the categories of data defined in section 35(8) of the Act except for the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual.

The Act regulates the processing of criminal court case information for a law enforcement purpose.

Data Protection Principles

How we meet comply with the principles set out in part 3 of the Data Protection Act 2018. As a data controller SCTS must demonstrate compliance with the data protection principles set out below:

Lawful and fair

SCTS will only undertake sensitive processing for law enforcement purposes where it has a lawful basis to do so and where the information is required for a specific reason.

We will communicate fair processing information to individuals through the SCTS website and will also make this available in other formats to individuals on request.

SCTS's processing of sensitive data for law enforcement purposes falls under the second and ninth conditions listed in Schedule 8 of the Act - administration of justice and archiving etc.

Purpose limitation

Sensitive processing will be restricted to only that which is necessary for the relevant law enforcement purpose, and it will not be used for a non law enforcement purpose unless that is authorised by law.

It may, however, be used for another law enforcement purpose by SCTS or another organisation that is authorised to carry out law enforcement processing.

SCTS will only share data processed for law enforcement purposes with another controller where SCTS is authorised by law to do so. We will document our lawful basis in data sharing agreements, any decision documents where we are sharing with another data controller on an ad hoc basis or policy documents covering data sharing with third parties.

SCTS does process and disclose law enforcement data for non-law enforcement. Further details can be found in the Appropriate Policy Document for UK GDPR purposes.

Data minimisation

Any personal data collected for law enforcement purposes will be restricted to that which is necessary for the purposes of processing.

Internal guidance, training and policies explain to staff that they should use the minimum amount of data required to enable specific tasks to be completed.

The SCTS Data Protection Impact Assessment process ensures only personal data and sensitive data strictly required is collected and processed by SCTS.

Accuracy

We will ensure as far as possible that the data we hold is accurate and kept up to date.

All staff are made aware of the need for accuracy and are responsible for the accuracy of the personal data they process.

Checks are carried out on the accuracy of data as part of post court checks and as part of monthly management checks.

Personal data found to be inaccurate will be rectified or erased whenever possible.

When necessary, the processing will be restricted in accordance with Sections 46 to 48 of the Act.

If inaccurate personal data has been disclosed, the recipient will be advised of this as soon as practicable.

Storage limitation

Aspects of every criminal court case are archived permanently by National Records of Scotland (NRS) under Public Records legislation.

All High Court of Justiciary case records are sent by SCTS in their entirety for permanent archiving to NRS after 10 years.

Records of Sheriff Court and Justice of the Peace court cases are either transmitted in line with the relevant Court Records Schedule after 25 years or destroyed in line with listed retention periods.

Security

SCTS has developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Technical Measures

SCTS applies information security standards this include encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password-controlled access, and end point management.

Organisational Measures

All staff are required to undertake yearly data protection compliance e-learning, access to data protection systems will be removed where data protection e-learning is not kept up to date.

All staff including contractors are vetted prior to appointment and must complete data protection compliance e-learning before access to systems is granted.

Buildings have physical security controls including key or swipe access to staff only areas.

Further measures include policy and guidance on:

- Data Security
- Data Sharing
- Records Management
- Retention and Destruction
- Physical Security

Review of this Policy

This policy document will be retained in accordance with Section 42 of the Act. It will be made available to the ICO on request.

The policy will be reviewed every two years (or more regularly if circumstances require it.