

# Data Protection

Standard Operating Procedure (SOP)

This SOP provides clear direction and procedural instruction to provide a consistency of response in accordance with force policy. It is recognised that policing is a dynamic profession and the standard response may not be appropriate in every circumstance. In every situation, your decisions and actions should be supported by the National Decision Model and based on the values and ethics of Police Scotland. You may be expected to provide a clear and reasonable rationale for any decision or action which you take.

## Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions

Owning Department: Chief Data Office / Information Assurance

Version Number: V10.00

Date Published: 19/02/2025

Contents

[Data Protection 1](#_Toc204850178)

[Notice: 1](#_Toc204850179)

[1. Introduction/purpose 4](#_Toc204850180)

[2. Training in Data Protection 4](#_Toc204850181)

[3. Data Protection Legislation 5](#_Toc204850182)

[4. Definitions under Data Protection Legislation 6](#_Toc204850183)

[5. Compliance with the Data Protection Principles 7](#_Toc204850184)

[Data Minimisation 8](#_Toc204850185)

[6. Lawfulness of Processing – GDPR Articles 6 and 9 9](#_Toc204850186)

[Special category data and criminal convictions data 9](#_Toc204850187)

[7. Use of Consent for Processing – GDPR 9](#_Toc204850188)

[8. Lawfulness of Processing – Law Enforcement 10](#_Toc204850189)

[8. Use of Consent for Processing – Law Enforcement 11](#_Toc204850190)

[10. Use of Law Enforcement Personal Data for a Non-Law Enforcement Purpose 11](#_Toc204850191)

[11. Privacy Notices 12](#_Toc204850192)

[12. Rights of the Data Subjects 13](#_Toc204850193)

[Subject Access Requests (SAR) 13](#_Toc204850194)

[Dealing with receipt of a SAR 14](#_Toc204850195)

[Information required for visa purposes 15](#_Toc204850196)

[Information required for employment purposes 15](#_Toc204850197)

[Other rights of data subjects 15](#_Toc204850198)

[13. Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default 16](#_Toc204850199)

[14. Data Processors 17](#_Toc204850200)

[15. Record of Processing Activities 17](#_Toc204850201)

[16. Roles and Responsibilities 18](#_Toc204850202)

[Senior Information Risk Owner (SIRO) 18](#_Toc204850203)

[Data Protection Officer (DPO) 18](#_Toc204850204)

[Other roles 19](#_Toc204850205)

[17. Personal Data Breaches 19](#_Toc204850206)

[18. Failure to Comply with the Provisions of the Data Protection Legislation 19](#_Toc204850207)

[19. Criminal Offences 19](#_Toc204850208)

[20. Accessing Police Scotland Systems 20](#_Toc204850209)

[Personal Data within Police Scotland Systems to which access is permitted 20](#_Toc204850210)

[Personal Data within Police Scotland Systems to which Access is not Permitted 21](#_Toc204850211)

[Personal Data Accessed Through Normal Working Practices 22](#_Toc204850212)

[21. Disclosure of Personal Data held within Police Scotland Systems 23](#_Toc204850213)

[22. Suspected Breaches of the Act – Section 170 to 173 23](#_Toc204850214)

[23. Concerns Regarding Conduct of Others 24](#_Toc204850215)

[24. How Officers and Staff obtain their Personal Data held by Police Scotland 25](#_Toc204850216)

[25. Monitoring 25](#_Toc204850217)

[Key Contacts 25](#_Toc204850218)

[Compliance record 26](#_Toc204850219)

[Version control table 26](#_Toc204850220)

[Feedback 28](#_Toc204850221)

## Introduction/purpose

This Standard Operating Procedure (SOP) supports the Police Service of Scotland, hereafter referred to as Police Scotland Data Protection Policy.

This SOP applies to:

* + - * Officers and staff within Police Scotland.
* Special constables.
* Temporary staff.
* Agency workers.
* Data processors of Police Scotland’s information
* Other individuals with authority to access Police Scotland information and information systems e.g. external project workers.

Collectively these will be referred to as employees throughout this SOP.

This SOP provides all employees with:

* Information regarding Data Protection (DP) legislation,
* Clear guidance on the correct use of personal data.
* Examples of misuse, and
* Details of the criminal offences under DP legislation that can be committed when personal data are misused.

## Training in Data Protection

All employees must receive mandatory induction training before being given access to information and Information Communications Technology (ICT) systems.

Anyone failing to attend the mandatory induction training, will not be provided with access to Police Scotland’s information and ICT systems.

All employees must successfully complete the DP refresher training course annually. The course is delivered in role-specific modules and is available on the Police Scotland Moodle training application. Officers and staff must select the module appropriate for the role that they undertake at the time of completion.

## Data Protection Legislation

The term ‘data protection legislation’ means:

* General Data Protection Regulation (GDPR) and its recitals;
* Data Protection Act 2018 (the Act); and
* Any regulations made under the Act.

The GDPR which was a European Union (EU) regulation, was incorporated into UK legislation following Brexit. It has been amended for UK use and named UK GDPR. While the Articles may have changed, the recitals at the beginning have not and therefore these should be taken as guidance only. The Act has also been amended to take account of the fact the UK is no longer part of the EU, but the name will not change.

Police Scotland must apply both the UK GDPR and the Act in the appropriate circumstances.

UK GDPR deals with the protection of individuals (data subjects) with regards to the general processing of personal data, which for ease of reference means it must be applied when dealing with personal data processed for non-law enforcement purposes. (The definitions of processing, law enforcement purposes and other data protection terms are provided below.)

UK GDPR applies for example, when dealing with the personal data of employees, disclosure of information to Social Work Departments by Concern Hubs and obtaining medical details during the custody process. General processing also applies to the processing of criminal convictions for non-law enforcement purposes, e.g. Vetting.

The Act however, deals with both general and law enforcement processing.

* Part 1 provides an overview of the Act, and definitions of some terms used in the Act.
* Part 2, supplements the UK GDPR with further definitions, exemptions and conditions to be satisfied.

A number of the Schedules to the Act also apply to general processing, providing further conditions which must be satisfied in certain circumstances, but the most commonly applied are Schedule 1 and Schedule 2. Therefore, the UK GDPR cannot be read and applied in isolation.

Part 3 of the Act deals with processing for law enforcement purposes. Schedule 7 and Schedule 8 also apply to law enforcement processing.

## Definitions under Data Protection Legislation

All processing of personal data must comply with the relevant parts of DP legislation.

The definitions of commonly used terms in relation to processing are as follows:

* + Controller means a person or legal person, public authority, agency or other body which alone or jointly with others, decides the purposes and means of processing of personal data. The Chief Constable is the controller for all personal data processed by Police Scotland.
  + Criminal convictions and offences or Related Security Measures includes personal data relating to:
  + the alleged commission of offences by the data subject, or
  + proceedings for an offence committed or alleged to have been committed by the data subject, or the disposal of such proceedings, including sentencing.
  + Data subject means the identified or identifiable living individual to whom personal data relates.
  + Identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to:
  + an identifier such as a name, ID number, location data or online identifier, or
  + one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
  + Law enforcement purposes are defined as the purposes of 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. Processing personal data for law enforcement purposes can only be carried out by competent authorities listed in Schedule 7 of the Act. Police Scotland is a competent authority.
  + Processing in relation to personal data is anything at all that we do with personal data, e.g. gathering, holding, accessing, altering, disclosing, deleting, etc.
  + Processor means a person or legal person, public authority, agency or body which processes personal data on behalf of the controller (other than an employee of the controller).
  + Personal data means any information relating to an identified or identifiable living individual.
  + Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.
  + Special/Sensitive Categories of data means processing of personal data revealing:
* racial or ethnic origin
* political opinions
* religious or philosophical beliefs
* trade union membership
* data concerning health
* data concerning an individual’s sex life or sexual orientation
* processing of genetic data or biometric data for the purposes of uniquely identifying an individual.

Generally, a photograph is not considered to be biometric data. It only becomes biometric data if “specific technical processing” is carried out. Usually this involves using the image data to create an individual digital template or profile, which in turn is used for automated image matching and identification. For other definitions see Article 4 of the GDPR and Part 2 and Part 3 of the Act.

## Compliance with the Data Protection Principles

Police Scotland must comply with data protection legislation guided by 7 data protection principles (Article 5 of the GDPR) which require that personal data is:

* + - * Processed fairly, lawfully and in a transparent manner.
      * Used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
      * Adequate, relevant, and limited to what is necessary.
      * Accurate and, where necessary, up to date.
      * Not kept for longer than necessary. Refer to the Record Retention SOP; and
      * Kept safe and secure. Refer to the Information Security SOP
      * Accountability - this principle requires Police Scotland to be able to evidence its compliance with the above six principles and make sure that it does not put individuals at risk because of the processing of their personal data. Failure to do so can result in breach of legislation, reputational damage, or financial implications due to fines. To meet its obligations, Police Scotland must put in place appropriate and effective measures to make sure it complies with data protection law.

### Data Minimisation

Officers and Staff must, when processing personal data ensure that it is:

* Adequate – sufficient to properly fulfil our stated purpose.
* Relevant – has a rational link to that purpose.
* Limited – to what is necessary – Police Scotland should not hold more than it needs for that purpose.

To assess whether Police Scotland are holding the right amount of personal data, it must first be clear about why we need it.

Officers and Staff should only collect personal data that they actually need to properly deliver Police Scotland’s specified purposes and should not collect additional unnecessary information.

Using the instructions in Record Retention SOP officers and staff must also periodically review the data they hold or for which they have responsibility and delete or instruct deletion of that which is not required.

Section 34 et seq. of the Act prescribe the principles relating to the processing of personal data for law enforcement purposes. They are the same as those above but with additions. Some of these are covered in more detail below.

There are differences between the GDPR and law enforcement principles. The reason for processing personal data must therefore be established to ensure the correct data protection legislation is applied.

## Lawfulness of Processing – GDPR Articles 6 and 9

In addition to complying with the principles, there are a number of conditions, at least one of which must be satisfied before personal data can be processed. These are listed in Article 6.

The most commonly used condition is Article 6.1(e), ‘processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller’, commonly referred to as ‘public task’. Further information of what constitutes a public task is provided in Section 8 of the Act.

The public task often arises from the Police and Fire Reform (Scotland) Act 2012, however, other conditions in Article 6 can and will apply to processing carried out by Police Scotland.

### Special category data and criminal convictions data

When processing special category data or criminal convictions data, a further condition from Article 9 must be satisfied in addition to one from Article 6. (Criminal convictions data can be processed under GDPR for non-law enforcement purposes such as vetting).

Once an Article 9 condition has been identified, Sections 10 and 11 and Schedule 1 of the Act must also be considered and applied appropriately.

## Use of Consent for Processing – GDPR

All other conditions for processing personal and special categories of personal data must be considered before consent.

The guidance is that as a public authority and an employer, Police Scotland should avoid the use of consent whenever possible due to the imbalance of power between the organisation and its employees or the public.

If it is identified that consent is the only lawful basis for processing, then careful consideration must be given as to why processing is required.

Information Assurance must be consulted before processing begins if it is believed consent is the most appropriate condition for processing.

Article 7 prescribes the conditions for processing using consent.

Consent of the data subject means any:

* Freely given.
* Specific.
* Informed and
* An unambiguous indication of the data subject’s wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

All of the above points must be satisfied for the consent to be valid. A data subject must also be able to withdraw consent as easily as they provided it, at no detriment to them.

Further guidance is provided on the Information Commissioner's Office website - Consent Guidance and should be read when considering using consent as the condition for processing.

## 8. Lawfulness of Processing – Law Enforcement

Section 35 of the Act states that processing personal data for law enforcement purposes must be lawful and fair, and that it will be lawful only to the extent that it is based on law and either:

1. the data subject has given consent to the processing for that purpose, or
2. the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

In addition, when the processing is of sensitive personal data, the processing is only permitted in one of two cases.

These are that the data subject has given consent to the processing or the processing is strictly necessary for law enforcement purposes, and the processing meets at least one of the conditions in Schedule 8.

For both of these conditions, at the time the processing is carried out an Appropriate Policy Document (APD) must be in place.

Police Scotland has the following APDs in place:

* APD Law Enforcement
* APD Non Law Enforcement

The lawful basis for processing for law enforcement purposes will often come from Section 20 (duties of a Constable), and Section 32 (Policing principles) of the Police and Fire Reform (Scotland) Act 2012. However, other legislation may also apply to the specific circumstances.

## **Use of Consent for Processing – Law Enforcement**

It is envisaged that using consent for law enforcement purposes will be relatively rare e.g. biometric data (which includes fingerprints) or biological samples, (blood, urine, saliva etc.) for elimination purposes.

When it does occur, the data subject must be informed in a clear and unambiguous manner about the voluntary nature of their agreement and must be given the possibility to withdraw it at any time.

If the data subject does withdraw consent, then the samples must be destroyed unless there is another legal basis for retaining them.

The consent of a data subject must be recorded and be subject of periodic review.

## Use of Law Enforcement Personal Data for a Non-Law Enforcement Purpose

Section 36 of the Act states that personal data collected for a law enforcement purpose may not be used for any other purpose unless that use is authorised by law.

This means that an Article 6 and, where appropriate, an Article 9 condition must be satisfied, and a compatibility test carried out as detailed in Article 6.4 of the GDPR.

## Privacy Notices

Police Scotland is required to provide information to data subjects with regards to how their data will be processed.

This is done by the means of a privacy notice. Article 13 of the GDPR and Section 44 of the Act provides details of what must be included in the notices. Police Scotland Privacy Notices are published on the Force website and as Force forms with the prefix 081-008.

When considering processing personal data for a purpose that is not already covered by a privacy notice, then either a current notice must be updated, or a new notice drafted.

Information on how to do this can be obtained from Information Assurance.

Police Scotland (Controller) may restrict, wholly or partly, the provision of information to the data subject to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to:

* Avoid obstructing an official or legal inquiry, investigation or procedure.
* Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.
* Protect public security.
* Protect national security.
* Protect the rights and freedoms of others.

Where the provision of information to a data subject is restricted, wholly or partly, the Controller must inform the data subject in writing without undue delay:

* That the provision of information has been restricted, (the Controller is not required to provide this information to the extent that the provision of the information would undermine the purpose of the restriction).
* Of the reasons for the restriction, (the Controller is not required to provide this information to the extent that the provision of the information would undermine the purpose of the restriction).
* Of the data subject’s right to make a request to the Commissioner under section 51.
* Of the data subject’s right to lodge a complaint with the Commissioner, and
* Of the data subject’s right to apply to a court under section 167.

Police Scotland will:

* Record the reasons for a decision to restrict (whether wholly or partly) the provision of information to a data subject, and
* If requested to do so by the Commissioner, make the record available to the Commissioner.

## Rights of the Data Subjects

The GDPR (Articles 15 to 19 and 21) and the Act (Sections 45 to 47) confer a number of rights on the data subjects.

These rights are:

* Right of access to their personal data held by Police Scotland by means of a Subject Access Request (SAR). There are certain exemptions to what will be disclosed to the data subject.
* Right to have inaccurate data rectified, this includes having incomplete personal data completed.
* Right to erasure of personal data (‘right to be forgotten’). This is particularly important when the processing has been based on the consent of the data subject.
* Right to restriction of processing.
* Right to object to processing. This right does not apply when the information is processed for law enforcement purposes.

### Subject Access Requests (SAR)

Article 15 of the GDPR, and Section 45 of the Act give to data subjects, the right to know whether or not their personal data is being processed by Police Scotland, and if so, access to that data and a number of other details which will be provided by Information Disclosure.

SARs can be made in writing via our online application form, by post, by email or by handing them in to any public facing police station, or they can be made verbally.

Further information is available online - Subject Access Requests - Police Scotland.

There is no charge associated with SARs.

### Dealing with receipt of a SAR

Information Disclosure has one month to respond to a SAR and the responses are often lengthy and time consuming to prepare.

Therefore, any SARs received by email or post must be forwarded immediately to dataprotectionsubjectacess@scotland.police.uk.

If an individual calls at a police station or approaches or calls any officer or staff member to submit a SAR, they should be encouraged wherever possible to complete the online form from their own device and advised that they will require to have scans or photographs of Identification Documents (ID) to hand.

Two forms of ID are required, which between them confirm the individual’s name, date of birth and current address - for example a passport, driving licence, birth certificate, utility bill, etc.

If an individual prefers to make the request verbally, the receiving officer should complete the online form for them, selecting ‘yes’ for the ‘I have authorisation’ question.

If an individual does not have ID with them but wishes to proceed regardless, the form can still be completed but they should be advised that the SAR will not be progressed until ID is received.

On completion of the form, the receiving officer should provide the individual with the unique reference number generated and advise them to send copies of their ID to Information Management (Disclosure), quoting their name and the reference number.

Emails can be sent to dataprotectionsubjectacess@scotland.police.uk and letters to Information Disclosure, Police Scotland, Second Floor, Woodhill House, Westburn Road, Aberdeen AB16 5GB.

Where the individual does have ID with them, it should be scanned (or photographed with a work device) and the originals returned to them immediately.

On submission of the form, the receiving officer will be directed to send an email with the scans/ photos attached to a dedicated email address.

### Information required for visa purposes

If the data subject requires the information for a visa application, they should be directed to the National Police Chief’s Council (NPCC) ACRO Criminal Records Office who will provide a certificate acceptable to Embassies.

### Information required for employment purposes

If the information is required for employment purposes, the data subject should be directed to Disclosure Scotland, Pacific Quay, Glasgow, G51 1YU, telephone 0870 609 6006 or, at www.mygov.scot/organisations/disclosure-scotland/ who will provide advice on what is available.

### Other rights of data subjects

Requests made for any of the other rights of the data subjects listed in section 12 above, are dealt with by Information Assurance. The response must be provided within one month.

The form to make such requests is on the Police Scotland website (Request for rectification, erasure, restriction or objection to processing of personal data (Form 081-010)). Should an applicant hand the request into a police station, the person receiving it should process as per SARs, but return it to the addresses listed on the form.

## Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default

Article 25 of the GDPR and Section 64 of the Act provide that Police Scotland has a legal obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into its processing activities.

Wherever a policy, project, system, process or initiative includes the processing of personal data, that processing must be compliant with data protection legislation at the point of delivery.

Where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of a data subject then a DPIA must be completed. This is a legal requirement.

The DPIA must be done at the very beginning of a project. This ensures that necessary changes can be made to the envisaged processing, rather than issues only being identified later in the project when making changes can be costly.

There are templates and guidance for DPIAs and these are:

* Forms Data Protection Impact Assessment - GDPR Processing – Guidance (Form 081-006(A)) and Data Protection Impact Assessment - GDPR Processing (Form 081-006) for GDPR processing.
* Forms Data Protection Impact Assessment - Law Enforcement Processing – Guidance (Form 081-007(A)) and Data Protection Impact Assessment - Law Enforcement Processing (Form 081-007) for law enforcement processing.

It is important that the guidance document is consulted and applied throughout the completion of the DPIA.

Part 1 of the template should be completed and emailed to Information.Assurance@scotland.police.uk who will decide whether the proposed processing is likely to result in a high risk to the rights and freedoms of data subjects. Information Assurance will record the reason for their decision. If there is no risk identified, then no further action is required in relation to the DPIA, although all other aspects should still be considered, e.g. security.

If a high risk is identified, Part 2 of the template must be completed and returned to IA. IA will assess the DPIA, provide advice and guidance to ensure the proposed processing meets the terms of data protection legislation and consult the Data Protection Officer who will review any associated risks with the processing, provide recommendations where relevant and advise whether the processing can proceed without referral to the Information Commissioner (ICO) for consultation as provided by s.65 of the Act.

## **Data Processors**

A processor is a person, legal person, public authority, agency or body which processes personal data on behalf of the controller (other than an employee of the controller).

When engaging a processor to carry out the processing of personal data on behalf of Police Scotland a Data Processing Agreement (DPA) must be completed. If a contract is dealt with by Procurement, a DPA must be completed as part of the contractual document set. Further guidance and support, including a template DPA can be obtained from Information Assurance.

## 15. Record of Processing Activities

Data protection legislation requires that a record is kept of the processing activities carried out by Police Scotland and provided to the Information Commissioner (ICO) on request.

If any new processing is envisaged, or it is intended to use personal data already held, for another purpose, then in addition to carrying out a DPIA (see paragraph 13), a record must be kept of the processing activities decided upon.

The record must contain the details listed in Article 30 of the GDPR for general processing and Section 44 of the Act for law enforcement processing. In Police Scotland, these details are primarily recorded in the Information Asset Register (IAR) and in the Data Catalogue.

All Strategic Information Asset Owners have access to the IAR and are responsible for ensuring the entries therein are up-to-date, supported by the Records Manager.

## 16. Roles and Responsibilities

We have an established Information Assurance network that ensures the risk to personal data across Police Scotland is identified and appropriately managed. The detailed roles and responsibilities comprise of the below:

### Senior Information Risk Owner (SIRO)

Police Scotland’s SIRO owns the overall risk arising from the processing personal data by Police Scotland. Our SIRO is the Assistant Chief Constable, Professionalism and Assurance.

### Data Protection Officer (DPO)

As a public authority, Police Scotland must have a Data Protection Officer (DPO).

Police Scotland’s Data Protection Officer (DPO) is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR and making recommendations to improve compliance. The role and tasks of the DPO are laid down in Articles 37 et seq. and Sections 69 et seq.

The name and contact details of the DPO must be published and communicated to the ICO. Data subjects can contact the DPO directly in relation to the processing of their personal data and to the exercise of their rights under the data protection legislation.

The Data Protection Officer can be contacted at [DataProtection@Scotland.police.uk](mailto:DataProtection@Scotland.police.uk)

### Other roles

Specific roles are assigned throughout our corporate hierarchy to manage personal data we process and the associated risks in terms of responsibilities, decision making and monitoring compliance.

Our detailed governance framework is contained within the Information Governance Standard Operating Procedure.

## 17. Personal Data Breaches

A personal data breach is defined as ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed’.

Certain personal data breaches must be reported to the ICO within 72 hours of it being discovered. Failure to do so may result in a substantial fine.

Anyone who identifies a personal data breach must report it immediately. Details of how to identify and report data breaches are in the Information Security SOP.

## 18. Failure to Comply with the Provisions of the Data Protection Legislation

Failure to comply with the data protection legislation can leave Police Scotland open to administrative fines by the ICO of up to £17.5m. Further details relating to fines are in Article 83 and Section 155 et seq. of the Act.

## 19. Criminal Offences

There are a number of criminal offences under the Data Protection legislation. These are detailed in Sections 170 to 173 of the Act.

It is a criminal offence for a person to knowingly or recklessly:

* Obtain or disclose personal data without the consent of the controller.
* Procure the disclosure of personal data to another person without the consent of the controller, or
* After obtaining the personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

It is a criminal offence to:

* Sell or offer to sell personal data held by Police Scotland.
* Knowingly or recklessly, without the consent of the controller to re-identify information which is personal data that has been previously de-identified.
* Alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure that a person making a subject access request would have been entitled to.

Any such actions by an employee will be investigated and may result in criminal proceedings and/or disciplinary action.

## 20. Accessing Police Scotland Systems

Personal data are processed by Police Scotland for:

* All aspects of policing.
* The provision of services to support policing
* The provision of administration and ancillary support to policing.

All officers and staff will receive training specific to the relevant systems and processes they use, and this may consist of on-the-job training.

### Personal Data within Police Scotland Systems to which access is permitted

Access to personal data within Police systems, whether held electronically or in manual records is permitted by Police Scotland to enable officers/employees to carry out their specific roles within their business areas.

The permission to access a system extends only to the specific records within that system which need to be accessed to allow officers and staff to carry out their role.

Certain employees, as part of their specific roles are permitted to access records of other employees of Police Scotland.

Examples of these are, Anti-Corruption Unit (ACU), Information Management, Professional Standards Department (PSD), People and Development (P and D), and ICT.

In all such cases, the access is limited to those records necessary for the purpose of carrying out the duties of the role.

Officers and staff may access their own SCoPE record and the SCoPE records for other personnel within Police Scotland for whom they have management responsibilities or when required for P and D or for administrative or business purposes.

### Personal Data within Police Scotland Systems to which Access is not Permitted

Employees do not have permission to access any record which is not necessary for the purposes of their job role. Accessing such records may constitute a criminal offence.

Such records include:

* Records of people known to them through their personal life, even if requested to by such a person; (see below relating to accessing such records through the normal course of the job role).
* Records to trace a person, vehicle or address for personal reasons.
* Records of any other police employee including their own; (but see reference to SCoPE record above).
* Accessing any record out of curiosity, or due to an interest in a specific type of case, e.g. sexual or violent, or because a case is high profile.

The term ‘personal life’ relates to their life outside the Force but is not intended to include a person with whom officers and staff have a passing acquaintance. It is not a chance meeting with a person which may be repeated from time to time.

If at all possible, officers and staff should not be allowed to be involved in an investigation relating to anyone known to them through their personal life, except in the role of a witness if necessary, and under no circumstances should they attempt to access the records of the investigation.

Should it be necessary for an officer or member of staff to be involved in an investigation of a person known to them through their personal life, e.g. where no one else is available, the relevant supervisor must allocate the investigation to another officer as soon as possible and record their reason. In any cases of doubt, guidance should be sought from PSD/ACU.

Any unauthorised attempts to access data, e.g. because a record is restricted, will be considered a breach of professional behaviour and may be investigated under the relevant conduct/disciplinary procedures. Police Scotland has the ability and right to monitor access or attempts to access the data it holds.

These controls are not designed to restrict officers and staff from performing their roles. A reasonable test to apply is to ask “Taking account of the instructions within this document, can I justify accessing this record for a specific lawful purpose?” If there is any doubt, then do not access the record. Instead guidance should be sought from the relevant line manager, PSD, ACU or Information Assurance.

### Personal Data Accessed Through Normal Working Practices

If during the course of carrying out their role, an officer or member of staff discovers that they have accessed the record of an individual known to them through their personal life, they must:

* Immediately log out of the record relating to that person.
* Bring it to the attention of their supervisor, and
* Provide them with evidence in support of why the record was accessed.

The supervisor will then allocate the work to another officer or member of staff unless it is not possible due to exceptional circumstances e.g. there is no one else available to whom the work can be allocated, and it cannot be delayed.

Permission to continue with the work must be authorised by an officer not below the rank of at least Inspector or by a police staff manager not below Grade 7, and at least one rank/grade above the individual concerned. The authorisation must be recorded and available in an auditable format.

The exception to the above guidance is when responding to a 999 call, when the call should be dealt with before taking the action above.

## 21. Disclosure of Personal Data held within Police Scotland Systems

Information must only be disclosed when it is lawful to do so. Unlawful disclosure can be a criminal offence, see section 19 above.

Officers and staff must be trained for their roles, as per section 20 above. This will include guidance, when relevant to the role, on sharing information routinely with a variety of external bodies/partner organisations such as Local Authorities.

When there is any question or doubt as to whether the information should be disclosed, advice must be sought from the relevant supervisor or Information Assurance.

It must not be assumed that because an external body/partner asks for the information, that they are entitled to have it. Further guidance can be obtained from the Information Sharing SOP and Information Assurance.

DP legislation does not apply to the personal data of deceased persons, but it does apply to the living relatives of, or other people who had been involved with the deceased. Care must be taken therefore not to breach the legislation by making unlawful disclosures regarding these persons when making disclosures relating to a deceased person.

## 22. Suspected Breaches of the Act – Section 170 to 173

All suspected breaches of the Act, will either be:

* Reported to the Crown Office and Procurator Fiscal Service (COPFS) Criminal Allegations Against the Police Department (CAAPD) or
* Will be dealt with in accordance with agreed protocols:
* For officers below the rank of Assistant Chief Constable, regardless of whether COPFS decides to prosecute, a breach of the Act can also constitute a breach of the Standards of Professional Behaviour and amount to misconduct or gross misconduct. Any such breach will be referred to PSD.
* For senior officers, i.e. Assistant Chief Constable, Deputy Chief Constable and Chief Constable, any suspected breach will be investigated by the Scottish Police Authority.
* For police staff a breach of the Act can also constitute a breach of the Disciplinary Procedure and/or the Code of Conduct. Any breach of the Code of Conduct will be investigated and assessed, and may make you liable to criminal and/or disciplinary action.

Breaches meeting the statutory threshold will also be reported to the Information Commissioner’s Office (ICO) in accordance with the Information Security SOP.

## 23. Concerns Regarding Conduct of Others

If an officer or member of staff has any concerns regarding the conduct of a colleague or a person known to them through their personal life, they must not access/attempt to access any records of that individual but instead they can use any of the following channels to report them:

* Through line management.
* Directly to ACU or PSD.
* Reported to the Crown Office and Procurator Fiscal Service (COPFS) Criminal Allegations Against the Police Department (CAAPD) or
* Through the Integrity Matters link on the intranet which also provides guidance on what should be reported. This can be done anonymously if preferred.
* Through Crimestoppers.

## 24. How Officers and Staff obtain their Personal Data held by Police Scotland

Officers and staff may access their own SCoPE record. If however, you want to know what other personal data is held by Police Scotland in relation to you:

* A request can be made to People and Development who will allow you to view your personnel file and will provide you with copies of up to 4 items from it.
* Officers/staff involved in a grievance or disciplinary process are permitted to see certain information. Please refer to the Policy Hub for further detail on these processes.
* A Subject Access Request (SAR) using Request for Access to Information (Form 052-002) and can be submitted, following the direction on the form. This is a statutory right. There is no charge for this.

## 25. Monitoring

Compliance with this instruction will be monitored via the DPO and the responsible teams reporting to Data Governance Board.

The Data Governance Board meets quarterly, chaired by the SIRO where matters of information management (including Data Protection matters), risk and assurance are subject of strategic consideration and decision making by SIRO.

## Key Contacts

Further advice and guidance regarding the contents of this SOP can be obtained from Information.Assurance@scotland.police.uk

## Compliance record

EqHIRA completion/review date: 12/02/2025

Information Management Compliant: Yes

Health and Safety Compliant: Yes

## Version control table

|  |  |  |
| --- | --- | --- |
| Version | History of amendments | Approval date |
| 1.00 | Initial Approved Version | 14/03/2013 |
| 2.00 | No change to content, updated to new template. | 04/11/2016 |
| 3.00 | Cyclical review. SOP fully rewritten. | 06/11/2017 |
| 4.00 | SOP rewritten to incorporate the Data Protection Act 2018 and the General Data Protection Regulation. | 23/05/2018 |
| 5.00 | Amendment to section 19 - changes to sections referred to under the Data Protection Act. | 06/11/2018 |
| 6.00 | General Data Protection Regulation links updated | 17/09/2019 |
| 7.00 | Hyperlinks to GDPR corrected in following paragraphs: 3.1, 4.3, 5.1, 6.1, 6.3, 7.4, 11.2, 11.3,12.1, 13.1, 14.2, 15.4, 18.2 and bullet point one in Appendix ‘A’. | 23/09/2019 |
| 8.00 | Content fully reviewed and rationalised in line with principles of SOP Review. | 01/06/2021 |
| 9.00 | Content fully reviewed and rationalised in line with principles of SOP review. Amended to incorporate regulatory recommendations regards accountability principle, restriction of privacy information, the role & responsibilities of the DPO and how to contact them a link to the management framework and information regards how compliance with the SOP will be monitored. | 12/02/2025 |
| 10.00 | Email updated P18. No other changes. Authorised by Policy manager. | 19/02/2025 |

## Feedback

All Police Scotland service delivery Policies, Standard Operating Procedures (SOPs) and National Guidance are subject to regular reviews. It is important that user feedback is considered when documents are reviewed.

If any officer / staff member wishes to provide comment, or make suggestions for improvements to this or any associated document, a Service Delivery Policy and Procedure Feedback Form (Form 066-014) should be used.