Privacy Information Notice

This Privacy Notice explains how and why South Yorkshire Police process your personal data, under UK GDPR , "general data" and DPA 2018 Part 3 "law enforcement data", the steps we take to keep your information safe and what to do if you have concerns as to how we have handled your data.

On the 25th May 2018 the UK produced its third generation of data protection law, the Data Protection Act 2018. This is the same date as the General Data Protection Regulation, GDPR, was launched throughout the European Union, EU. Following withdrawal from the EU on 1st January 2021, the EU GDPR will be adopted into UK law by section 3 of the EU Withdrawal Act 2018 (EUWA 2018) and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (Implementing Regulations). This part of the UK's post transition data protection law will be known as 'UK GDPR', which can be found at Part 2 of the Data Protection Act 2018.

'UK GDPR' will apply the EU's GDPR standards for the processing of data considered as "general data"; this is data which is processed for a reason not involving law enforcement or national security. This does include some processing for a policing purpose as defined in Management of Police Information 2005 as 'protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice, and any duty or responsibility of the police arising from common or statute law.'

Part 3 of the Data Protection Act 2018 (DPA 2018), implements the Law Enforcement EU Directive (Directive 2016/680) and is separate from the UK GDPR/GDPR. The processing of personal data for law enforcement purposes can only be done by an organisation which is considered as a "competent authority" in law. Law enforcement purposes are "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". How organisations should process data for "law enforcement purposes" can be found at Part 3 of the Data Protection Act 2018.

Who are we?

South Yorkshire Police is the territorial police force responsible for policing the areas of South Yorkshire in North East England.

The Chief Constable – **Lauren Poultney** of South Yorkshire Police is the **Data Controller** and as such has overall responsibility for the lawful processing of all personal data processed by the force. She is assisted by the **Data Protection Officer** who provides advice and guidance in relation to data protection law. Our data protection registration number is Z572421X which is renewed each year.

If you have any questions about how we use your personal information, our DPO can be reached by the Information Compliance email at informationcompliance@southyorks.pnn.police.uk, or by post at South Yorkshire Police, Data Protection Officer, Information Compliance Department, Unit 20, Churchill Way, Sheffield, S35 2PY.

South Yorkshire Police documents:

- The purposes of our processing
- The categories of individuals whose data we process
- The categories of personal data that we process
- The categories of recipients of personal data
- Details about any overseas transfers
- Our retention schedules for the different categories of personal data

Law Enforcement - Processing under Part 3 DPA 2018

Why do we process your personal information for law enforcement purposes?

When South Yorkshire Police processes your personal data for the Law Enforcement Purpose it does so as a Competent Authority acting under the official authority of the Chief Constable to prevent, investigate, detect or prosecute criminal offences or to execute criminal penalties, including the safeguarding against and the prevention of threats to public security.

Whose personal data do we process for law enforcement purposes?

In order to carry out the Law Enforcement Purpose, South Yorkshire Police may collect, record, organise, structure, store, adapt, alter, retrieve, consult, use, disclose by transmission, dissemination or otherwise making available, align or combine, restrict, erase or destroy the personal information relating to a wide variety of individuals including but not limited to:

- Offenders and suspected offenders;
- Witnesses or reporting persons;
- Individuals passing information to South Yorkshire Police;
- Victims, both current, past and potential, and
- Other individuals necessarily identified in the course of law enforcement investigations and prosecutions, execution of criminal penalties or during the safeguarding against and the prevention of threats to public security

What type of personal information do we process?

In order to meet the Law Enforcement Purpose we will process varying types of personal data, this includes:

Information relating to natural persons who can be identified or who are identifiable, directly from the information in question or who can be indirectly identified from that information in combination with other information.

Special Category Personal Data:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);

data concerning **health**;

- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Criminal Offence data

Personal data relating to criminal convictions and offences or related security measures and 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.

This might include but is not limited to:

Your name and address; Employment details; Financial details; Criminal proceedings, Outcomes and sentences; Cautions; Physical identifiers including DNA, fingerprints, and other genetic samples; Photograph, Sound and visual images; Criminal Intelligence; Information relating to safety; Incidents, and Accident details.

We will use only the minimum amount of personal information necessary to fulfil a particular purpose or purposes. Personal information can be information that is held on a computer, in a paper record such as a file or images, but it can also include other types of electronically held information such as CCTV images.

Where do we get the personal information from?

Other law enforcement agencies; HM Revenue and Customs; International law enforcement agencies and bodies; Licensing authorities; Legal representatives; Prosecuting authorities; Solicitors; Courts; Prisons and Young Offender Institutions; Security companies; Partner agencies involved in crime and disorder strategies; Private sector organisations working with the police in anti-crime strategies; Voluntary sector organisations; Approved organisations and people working with the police; Independent Office for Police Conduct; Her Majesty's Inspectorate of Constabulary; Governmental agencies and departments; Emergency services such as the Fire and Rescue Services, National Health Service or Ambulance; Persons arrested; Victims; Witnesses; Relatives, guardians or other persons associated with the individual; South Yorkshire Police CCTV systems; Body worn video, DASH CAMS, Handheld cameras, drones and footage provided by the public and from other communications and correspondence sent to us.

There may be times where we obtain personal information from sources such as other police services and our own police systems such as our local information system.

What is our lawful basis for processing your personal data?

South Yorkshire Police process your personal data as a Competent Authority for the Law Enforcement Purpose under DPA 2018:

S35This section has no associated Explanatory Notes (1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.

S35 (2) The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a)the data subject has given consent to the processing for that purpose, or

(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority. This section has no associated Explanatory Notes

Sensitive Processing shall occur only in two cases:

The first case is where—

(a)the data subject has given consent to the processing for the law enforcement purpose as mentioned in subsection (2)(a), and

(b)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

The second case is where—

(a)the processing is strictly necessary for the law enforcement purpose,

(b)the processing meets at least one of the conditions in Schedule 8, and

(c)at the time when the processing is carried out, the controller has an appropriate policy document in place (see section 42).

Your personal data is collected for a specified, explicit and legitimate Law Enforcement Purpose, and, any new processing will not be incompatible with the purpose for which it was originally collected.

How do we handle your personal information?

We handle personal information according to the requirements of Part 3 of the Data Protection Act 2018. Your personal information held on our systems and in our files is secure and is accessed on a "need to know" basis by our staff, police officers, or data processors working on our behalf.

Where we are processing personal data for Law Enforcement Purpose we will ensure that any personal data is:

- Processed lawfully and fairly;
- Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with the purpose for which it was originally collected;
- Adequate, relevant and not excessive in relation to the purpose for which it is processed;
- Accurate and, where necessary, kept up to date, and;
- Every reasonable step is taken to ensure that personal data is accurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay;
- Kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits have been established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes;
- 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)."

We will strive to ensure that any personal information used by us or on our behalf is of the highest quality in terms of accuracy, relevance, and adequacy and will not be excessive. We will attempt to keep it as up to date as possible and will protect your data from unauthorised access or loss.

We will regularly review your data to ensure it is still required and we have a lawful purpose to continue to retain it. If there is no lawful purpose then your data will be securely destroyed.

Who do we share your personal information with?

To enable South Yorkshire Police to meet their statutory duty we may be required to share your data with other organisations that process data for a similar reason, in the UK and/or overseas, or in order to keep people safe.

These organisations include:

- Other law enforcement agencies (including international agencies);
- Partner agencies working on crime reduction or safeguarding initiatives;
- Partners in the Criminal Justice arena;
- Local government;
- Authorities involved in offender management;

- International agencies concerned with the safeguarding of international and domestic national security;
- Third parties involved with investigations relating to the safeguarding of national security; and
- Other bodies or individuals where it is necessary to prevent harm to individuals. The UK has implemented the GDPR; and the Law Enforcement Directive is transposed in full within Part 3 of the UK's Data Protection Act 2018. The UK therefore continues to meet the same data protection standards as European counterparts.
- Insurance bodies for fraud investigation

The Chief Constable of South Yorkshire Police and Controllers in EU Member States can continue to share law enforcement data under the mechanisms provided for in Article 37(1) of the Law Enforcement Directive.

South Yorkshire Police will also disclose personal information to other bodies or individuals when required to do so, or under an act of legislation, a rule of law, and by court order. This may include and is not limited to:

- Home Office
- Other Competent Authorities including those in Foreign jurisdictions
- Serious Fraud Office
- National Fraud Initiative
- Courts
- Crown Prosecution Service

How do we keep your personal information safe?

South Yorkshire Police takes the security of all personal information under our control very seriously. We will comply with the relevant parts of the legislation relating to security, and seek to comply with the College of Policing Information Assurance authorised practice, and relevant parts of the ISO27001 Information Security Standard.

We will ensure that appropriate policy, training, technical and procedural measures are in place. These will include, but are not limited to, ensuring our buildings are secure and protected by adequate physical means. The areas restricted to our police officers and staff, are only accessible by those holding the appropriate identification, and have legitimate reasons for entry. We carry out audits of our buildings security to ensure they are secure. Our systems meet appropriate industry and government security standards.

We carry out regular audits and inspections, to protect our manual and electronic information systems from data loss and misuse, and only permit access to them when there is a legitimate reason to do so. Our standard operating procedures and policies contain strict guidelines as to what use may be made of any personal information contained within them. These procedures are reviewed regularly to ensure our security of information is kept up-to-date.

Some of the bodies or individuals to which we may disclose personal information are situated outside of the UK or European Union - some of which do not have laws that protect data protection rights as extensively as in the United Kingdom. If we do transfer personal data to such territories, we undertake to ensure that there are appropriate safeguards in place to certify that it is adequately protected as required by the legislation.

How long will you keep my personal information?

South Yorkshire Police keeps your personal information as long as is necessary for the particular purpose or purposes for which it is held. Personal information which is placed on the Police National Computer is retained, reviewed and deleted in accordance with the Retention Guidelines for Nominal Records on the Police National Computer

Other records that contain your personal information and which was processed for law enforcement purposes are retained in accordance with the College of Policing guidance on the Management of Police Information, MoPI, and South Yorkshire Police's Information Management Policy in line with the NPCC National Retention Schedule.

What are my Rights?

A key area of change in the new Data Protection Act relates to individuals' rights, the law refreshers existing rights by clarifying and extending them and introduces new rights.

However, your information rights will be dependent on the reason why and how the data was collected and why it is being used.

Your information rights in relation to your personal data processed for law enforcement purposes are:

Right to be Informed - This places an obligation upon south Yorkshire Police to tell you how we obtain your personal information and describe how we will use, retain, store and who we may share it with.

We have written this Privacy Notice to explain how we will use your personal information and tell you what your rights are under the legislation.

Right of Access - This is commonly known as subject access and is the right which allows you access to your personal data and supplementary information, however it is subject to certain restrictions.Rights of access do not apply to the processing of 'relevant personal data' , we can limit confirmation that we are processing data and any access to personal data, if necessary and proportionate in order to:

- Avoid obstruction to an official or legal inquiry, investigation or procedure;
- Avoid prejudicing prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
- Protect public security; or
- Protect the rights and freedoms of others.

Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority. Access to 'relevant personal data' is governed by the appropriate legislation covering the disclosure of information in criminal proceedings, such as (in England and Wales) the Criminal Procedure and Investigations Act 1996.

The request must be processed within one month. Where a request is refused the individual must be notified and where no action is taken individuals have the right to be informed of how to seek a judicial remedy.

Right to Request Rectification - You are entitled to have personal data rectified if it is inaccurate or incomplete. We can refuse this request where the data is necessary and proportionate or relates to 'relevant personal data' i.e. to avoid obstructing an official or legal inquiry, investigation or procedure, or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, as detailed above.

Right to Erasure and Right to Restriction - You have the right to request the deletion or removal of your personal data and/or the right to 'block' or restrict the processing of your personal data where

there is no compelling reason for its continued processing. We can refuse such a request where it is necessary and proportionate or relates to 'relevant personal data', i.e. to avoid obstructing an official or legal inquiry, investigation or procedure or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, as detailed above. The erasure of personal data relating to criminal offences cannot be considered until its full period of retention has been reached.

Rights Relating to Automated Decision Making - Automated individual decision making and profiling is a decision made by automated means without any human involvement.

Should you wish to learn more about your information rights or how to make an Information Rights Request please follow the link below:

Your Data Rights

General Processing under UK GDPR

Why do we process your personal information, considered as general data?

South Yorkshire Police process personal information for a variety of reasons which are not related to law enforcement.

For example we process personal data for the following "**lawful purposes**" to;

- Assist us in meeting our "**Legal Obligations**" as employers,
- To manage "**Contracts**" with those who supply us with goods and services,
- To help us support those who we come into contact with, which can be done by obtaining their "**Consent**", or due to our "**Legitimate Interests**", this includes processes to improve the service we provide the public.
- To perform tasks which are considered as being in the "**Public Interest**"
- The provision of ancillary services to support the Law Enforcement Purposes which includes:
- Staff/pension administration, occupational health and welfare;
- Management of public relations, journalism, advertising and media;
- Management of finance, payroll, benefits, accounts, audit, internal review;
- Internal review, accounting and auditing;
- Training;
- Property management;
- Insurance management;
- Vehicle and transport management;
- Payroll and benefits management;
- Management of complaints;
- Vetting;
- Management of information technology systems;
- Legal services;
- Information provision;

- Licensing and registration;
- Pensioner administration;
- Research including surveys;
- Performance management;
- Sports and recreation;
- Procurement;
- Planning;
- System testing and fault resolution;
- Security;
- Health and safety management

See the Covid-19 privacy notice for more information about how we may seek to collect and hold additional information about you in relation to the challenges we are all facing during the Coronavirus pandemic.

South Yorkshire Police is required to conduct Customer Satisfaction Surveys to evaluate our performance and effectiveness. We may contact individuals, such as victims of crime or those reporting incidents, and ask them to give us their opinion of the services we are providing to the public. We use the information given to improve our service and like many police forces use a private company to undertake such surveys on our behalf with strict controls to protect the personal data of those involved.

Whose personal data do we process for General purposes?

- Police Officers
- Complainants, correspondents and enquirers;
- Advisers, consultants and other professional experts;
- Suppliers;
- Current and former staff including volunteers, agents, temporary and casual workers;
- Former and potential members of staff, pensioners and beneficiaries;
- Individuals that have been in contact with us
- External stakeholders
- Partner agencies

What type of personal information do we process?

Information relating to natural persons who can be identified or who are identifiable, directly from the information in question or who can be indirectly identified from that information in combination with other information.

Special Category Personal Data

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;

- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Criminal Offence data

Personal data relating to criminal convictions and offences or related security measures and 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.

The type of personal information we hold will vary depending upon the reason you have had contact with us but it may include:

Your name and address; Biometrics such as Fingerprints, DNA or other genetic samples, Photograph; Family, lifestyle and social circumstances; Education and training details; Employment details; Financial details; Goods or services provided; Offences and alleged offences; Criminal proceedings, outcomes and sentences; Sound and visual images; References to manual records or files; Information relating to safety and health; Complaint, incident, civil litigation and accident details, Licenses or permits held, Criminal Intelligence.

We will use the minimum amount of personal information necessary to fulfil a particular purpose. Your personal information may be held on a computer system, in a paper record such as in a physical file or a photograph.

Where do we get the personal information from?

To carry out the purposes we have described we may obtain personal information from a wide variety of sources, including:

Other law enforcement agencies , International law enforcement agencies and bodies; HM Revenue and Customs; Licensing authorities; Legal representatives; Prosecuting authorities; Solicitors; Courts; Voluntary sector organisations; Independent Office for Police Conduct; Her Majesty's Inspectorate of Constabulary; Auditors; Police and Crime Commissioners; Central government, governmental agencies and departments; Relatives, guardians or other persons associated with an individual; Current, past or prospective employers of the individual; Healthcare, social and welfare advisers or practitioners; Education, training establishments and examining bodies; Business associates and other professional advisors; Employees, officers and agents of South Yorkshire Police; Suppliers, providers of goods or services; Persons making an enquiry or complaint; Financial organisations and advisors; Credit reference agencies; Survey and research organisations; Trade union, staff associations and professional bodies; Local government; Voluntary and charitable organisations; Ombudsmen and regulatory authorities; The media, Prisons, Probation Services, Security Companies, Partner agencies involved in crime and disorder strategies; Private sector organisations working with the police in anti-crime strategies; Approved organisations and people working with the police; Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS); Emergency services; Data Processors working on behalf of Derbyshire Constabulary. ANPR (Automatic Number Plate Recognition)

South Yorkshire Police may also obtain personal data from other sources such as its own CCTV systems, Body Worn Video footage or correspondence.

What is our lawful basis for processing your personal data?

Personal data shall be processed fairly, in a transparent manner and lawfully and, in particular, shall not be processed unless at least one of the lawful basis for processing exists under Article 6 of the GDPR.

Our lawful bases for processing are:

(a) Consent: you have given clear consent for us to process your personal data for a specific purpose. Where we rely on your consent to process data, you have the right to withdraw this at any time.

(b) Contract: the processing is necessary for a contract that we have with you, or because you have asked us to take specific steps before you enter into a contract.

(c) Legal obligation: the processing is necessary for South Yorkshire Police to comply with the law.

(d) Vital interests: the processing is necessary to protect your's or someone else's life.

(e) Public task: the processing is necessary for South Yorkshire Police to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect your personal data which overrides those legitimate interests.

Most of the processing that we do (outside of Law Enforcement processing) falls under 6(1)(e) – public task – because much of what we do is based in law.

When we process any of your Special Category Personal Data we shall process it fairly, in a transparent manner and lawfully, and, in particular, we shall not be processed unless at least one of the lawful basis for processing exists under Article 6 of the GDPR and a separate condition for processing special category data under Article 9 or a condition in DPA 2018 Schedule 1 is met.

Criminal offence data will be processed fairly, in a transparent manner and lawfully. It will not be processed for a non-law enforcement purpose unless authorised in law or under the official authority of the Chief Constable and at least one of the lawful basis for processing exists under GDPR Article 6 and a separate condition for processing special category personal data under Article 9 is met condition and a condition in DPA 2018 Schedule 1 is met and the processing will also comply with Article 10.

How do we handle your personal information?

We handle personal information according to the requirements of Part 2 of the UK Data Protection Act 2018 and UK GDPR which applies the EU's General Data Protection Regulation, GDPR, standards for the processing of data considered as "general data". Your personal information, held on our systems and in our files, is secure and is accessed by our staff, police officers, contractors and data processors working on our behalf, outsourced providers in accordance with their contract and volunteers when required to do so for a lawful purpose.

Where we are processing data for the General Purposes we will ensure that any personal data is:

- Processed lawfully, fairly, in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

We will ensure that your personal information is handled fairly and lawfully. We will strive to ensure that any personal information used by us or on our behalf is of the highest quality in terms of accuracy, relevance, and adequacy, is not excessive and is kept as up to date as possible and is protected appropriately. We will review to ensure it is still required and is lawful for us to continue to retain it and when no longer required for any purpose detailed in this notice, we will securely destroy it.

We will review your data to ensure it is still required and we have a lawful purpose to continue to retain it. If there is no lawful purpose then your data will be securely destroyed.

We will respect your information rights under the DPA Act 2018 and UK GDPR/GDPR.

Who do we share your personal information with?

To carry out the purposes described South Yorkshire Police may disclose personal information to a wide variety of recipients including those from whom personal data is obtained. This may include:

- Support Services for Victims and Offenders;
- To bodies or individuals working on our behalf such as IT contractors or survey organisations;
- Local government;
- Central government;
- Ombudsmen and regulatory authorities;
- Survey and research organisations;
- The media;
- Health Care Providers Businesses (including security companies, and other supplies of goods and services) and Other private sector organisations working with the police in anti-crime strategies agencies and other third parties concerned with the safeguarding of and investigation relating to international and domestic national security

- Local authorities, national and local government departments and agencies (including the Home Office, HM Revenue and Customs, the Serious Fraud Office, the Child Maintenance Service, the National Fraud Initiative, and private safeguarding agencies)
- Police and Crime Commissioners
- Legal representatives, prosecuting authorities, courts, prisons, and other partners in the criminal justice arena
- Bodies or individuals working on our behalf
- Ombudsmen, auditors and regulatory authorities
- Other bodies or individuals where required under any legislation, rule of law, or court order

Where you have provided your personal data to us for the purposes of the police constable recruitment process, your data, including biographical monitoring information, will be shared with the College of Policing.

It will be stored on their secure network or within their Assessment Information Management System (AIMS). From this information, your name, email address and candidate reference number will be uploaded to the new online assessment platform for constable recruitment and shared with the third party provider hosting the system in order to progress your application virtually.

We may also disclose to other bodies or individuals where necessary to prevent harm to individuals. Disclosures of personal information is considered on a case-by-case basis, using only the personal information appropriate to a specific purpose and circumstances, and with necessary controls in place.

Disclosures of personal information are made on a case-by-case basis, only relevant information, specific to the purpose and circumstances, will be disclosed and with necessary controls in place.

South Yorkshire Police will also disclose personal information to other bodies or individuals when required to do so, this could be under an act of legislation, by a rule of law, or by court order. This may include:

- Child Maintenance Service;
- Children and Family Courts Services;
- Home Office;
- Courts;
- Any other Regulatory Body who can demonstrate that there is a legitimate purpose for the processing of your personal data.

South Yorkshire Police may also disclose personal information on a discretionary basis for the purpose of, and in connection with, any legal proceedings or for obtaining legal advice.

How do we keep your personal information safe?

South Yorkshire Police takes the security of all personal information under our control very seriously. We will comply with the relevant parts of the legislation relating to security, and seek to comply with the College of Policing Information Assurance authorised practice, and relevant parts of the ISO27001 Information Security Standard.

We will ensure that appropriate policy, training, technical and procedural measures are in place. These will include, but are not limited to, ensuring our buildings are secure and protected by adequate physical means. The areas restricted to our police officers, staff and partner agencies staff is only accessible by those holding the appropriate identification, and have legitimate reasons for entry. We

carry out audits of our buildings security to ensure they are secure. Our systems meet appropriate industry and government security standards.

We carry out regular audits and inspections, to protect our manual and electronic information systems from data loss and misuse, and only permit access to them when there is a legitimate reason to do so. Our standard operating procedures and policies contain strict guidelines as to what use may be made of any personal information contained within them. These procedures are reviewed regularly to ensure our security of information is kept up-to-date.

Some of the bodies or individuals to which we may disclose personal information are situated outside of the UK. If we do transfer personal data to such territories, we undertake to ensure that there are appropriate safeguards in place to certify that it is adequately protected as required by the legislation.

How long will you keep my personal information?

South Yorkshire Police keeps your personal information as long as is necessary for the particular purpose or purposes for which it is held. Personal information is retained and deleted in line with the South Yorkshire Police's Information Management Policy and Force Retention Schedule.

What are my information rights?

Your information rights in relation to personal data considered as "general data" are:

Right to be Informed - This places an obligation upon South Yorkshire Police to tell you how we obtain your personal information and describe how we will use, retain, store and who we may share it with.

We have written this Privacy Notice to explain how we will use your personal information and tell you what your rights are under the legislation

Right of Access - This is commonly known as subject access and is the right which allows you access to your personal data and supplementary information, however it is subject to certain restrictions.

Rights of access do not apply to the processing of 'relevant personal data', we can limit confirmation that we are processing data and any access to personal data, if necessary and proportionate in order to:

- Avoid obstruction to an official or legal inquiry, investigation or procedure;
- Avoid prejudicing prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
- Protect public security; or
- Protect the rights and freedoms of others.

Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority. Access to 'relevant personal data' is governed by the appropriate legislation covering the disclosure of information in criminal proceedings, such as (in England and Wales) the Criminal Procedure and Investigations Act 1996.

The request must be processed within one month, or three months in complex cases. Where a request is refused the individual must be notified and where no action is taken individuals have the right to be informed of how to seek a judicial remedy.

Right to Request Rectification - You are entitled to have personal data rectified if it is inaccurate or incomplete. We can refuse such a request where it is necessary and proportionate or relates to 'relevant personal data', i.e. to avoid obstructing an official or legal inquiry, investigation or procedure or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, as detailed above.

Right to Erasure - The right to erasure is also known as 'the right to be forgotten'. This right enables you to request the deletion or removal of personal data where there is no compelling reason for its continued processing. We can refuse such a request where it is necessary and proportionate or relates to 'relevant personal data', i.e. to avoid obstructing an official or legal inquiry, investigation or procedure or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, as detailed above. The erasure of personal data relating to criminal offences cannot be considered until its full period of retention has been reached.

Right to Restrict Processing - Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, organisations are permitted to store the personal data, but not further process it. We can refuse such a request where it is necessary and proportionate or relates to 'relevant personal data', i.e. to avoid obstructing an official or legal inquiry, investigation or procedure or to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, as detailed above.

Right to Data Portability - The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services.

Right to Object - Individuals have the right to object to:

- The processing of your personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- The processing of their personal data for direct marketing (including profiling); and
- **The processing of their personal data for the purposes of scientific/historical research and statistics**.

Rights Relating to Automated Decision Making - Automated individual decision making and profiling is a decision made by automated means without any human involvement.

Should you wish to learn more about your information rights or how to make Information Rights Request please see the link below:

Your Data Rights

Automated Decision Making Including Profiling

Automated decision-making means making a decision about you solely by automated means without any human involvement.

Profiling means automated processing of your personal data to evaluate certain things about you.

South Yorkshire Police will only use automated decisions including profiling where:

- For contractual reasons and where we have carried out a data protection impact assessment, or
- You have explicitly consented, or
- We are authorised by law and this is the most appropriate way to achieve our aims.

Where an automated decision has been made about you, including profiling there will be a right of review.

How to make a complaint to the Information Commissioner

The Information Commissioner is the independent Authority responsible within the UK for ensuring we comply with data protection legislation. If you have a concern about how we have used your personal information or you believe you have been adversely affected by our handling of your data, please make contact with us so as we can try to rectify.

Alternatively, you may wish to contact the Information Commissioner's Office using the information below:

Their Helpline
0303 123 1113
(Their normal opening hours are Monday to Friday between 9am and 5pm)

Their email
casework@ico.org.uk

Their address
Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Monitoring

South Yorkshire Police may monitor or record and retain telephone calls, texts, emails and other electronic communications to and from the force in order to deter, prevent and detect inappropriate or criminal activity, to ensure security, and to assist the purposes described above. South Yorkshire Police does not place a pre-recorded 'privacy notice' on telephone lines that may receive emergency calls (including misdirected ones) because of the associated risk of harm that may be caused through the delay in response to the call.

Cookies

South Yorkshire Police use a number of different cookies on this website.

Changes to our Privacy Notice

We keep our privacy notice under review.

If we plan to use your personal information for a new purpose we will update our privacy notice and communicate the changes before we start any new processing.