Privacy Notice: Surrey Police and Sussex Police
Force Privacy Notice

Surrey Data Protection Officer: **Kelly Thornton**
dataprotection@surrey.police.uk

Sussex Data Protection Officer: **Martin Brazier**
DPO@sussex.police.uk

Our Privacy Notice tells you how Surrey Police and Sussex Police holds, retains, processes, discloses and shares the information we obtain about you. It also explains the rights you have regarding your personal information.

The use and disclosure of your personal information is governed in the United Kingdom by UK Data Protection Legislation. The Data Protection Act 2018 require organisations to process data in a fair, lawful and transparent manner. It mandates that certain information must be communicated to data subjects to ensure that they are as well informed as possible about how their data will be processed.

The Chief Constables for Surrey Police and Sussex Police are defined as the 'Data Controllers' for the purposes of the legislation and are required to ensure Surrey Police and Sussex Police handles all personal information in accordance with that legislation.

Surrey Police and Sussex Police takes that responsibility very seriously and takes great care to ensure your personal data is processed appropriately to maintain your trust and confidence in the police.

This privacy notice explains:

- how we collect, store, use, disclose, retain and destroy personal data through the website (those activities are also referred to as processing personal data)
- the steps we take to ensure personal data we process is protected properly
- the rights individuals have when we process their personal data

We will treat information you provide to us in using this website treated in confidence and we will not disclose it to third parties unless we are required to do so by law, or as explained in this privacy notice

What is personal data?

Personal data is any information we handle that relates to an identified or identifiable natural person. An 'identifiable natural person' is anyone who can be identified, directly or indirectly from information, including by reference to a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Our Contact Details and Data Protection Officer

Our Information Management Team manages our data protection compliance. We take our data protection responsibilities seriously. We take great care to ensure we process your personal data properly to maintain your trust and confidence. You can contact our Data Protection Officer (DPO) if you have any questions or concerns about how we process your personal data.

Email	**Surrey**	dataprotection@surrey.police.uk		
	Sussex	DPO@sussex.police.uk		
Address	**Surrey**	Surrey Police PO Box 101 Surrey Guildford GU1 9PE	**Sussex**	Sussex Police Headquarters Church Lane Lewes East Sussex BN7 2DZ

Why do we process your personal data?

We have a legal duty to uphold the law, prevent crime, bring offenders to justice, and protect the public. To do this we process your personal information for carrying out a range of activities commonly known as the 'policing purpose'. These include:

- preventing and detecting crime
- apprehending and prosecuting offenders
- protecting life and property
- preserving order
- maintaining law and order
- assisting the public
- safeguarding national security
- defending civil proceedings
- fulfilling any other police duties or responsibilities arising under common or statute law

We also process personal data for purposes in support of the policing purpose. These include: recruitment; administration of current and former employees, contractors, and volunteers; property and asset management; financial management; media relations management, complaints handling; victim support; research, including surveys; and provision of educational programmes and support.

Whose personal data do we process?

We process information relating to a range of individuals, including:

- victims of crime
- witnesses to crime
- people convicted of an offence
- people suspected of committing an offence
- complainants, correspondents and enquirers
- advisors, consultants and other professional experts
- suppliers
- current and former employees, cadets, agents, temporary and casual workers, and volunteers
- representatives of individuals in this list, such as parents, other relatives, guardians, and people with power of attorney

What types of personal data do we process?

The type of personal information we hold will vary depending upon the reason you have had contact with us but it may include: the categories below and could include Special Category data and Criminal Offence data.

We may process personal data relating to or consisting of the following categories:

- personal details (such as name, address and biographical details)
- family, lifestyle and social circumstances
- education and training details
- racial or ethnic origin
- political opinions
- religious or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition, both declared and suspected
- sexual life
- offences (including alleged offences)
- criminal proceedings, outcomes and sentences
- physical identifiers (including DNA, fingerprints and other genetic or biometric samples)
- sound and visual images (e.g. from body worn cameras, CCTV, or facial recognition software)
- financial details
- goods or services provided
- licences or permits held (e.g. driving licences or firearms certificates)
- criminal intelligence
- information identifying user vulnerability, persistent targeting, and/or hate crime status
- references to manual records or files
- information relating to health and safety
- complaint, incident, and accident details
- opinions and assessments of officers and staff in relation to individuals dealt with

The types of personal data we process will vary depending on the purpose. We aim to process the minimum amount of personal data necessary for the relevant purpose. Your Personal information may be held on a computer system, in a paper record such as in a physical file or a photograph but it can also include other types of electronically held information. You should not assume that we hold personal data in all of the categories identified for every person whose personal data we process.

Where do we get the personal data we process?

We collect personal data from a variety of sources, including:

- individuals who visit the website and interact with it (including by filling in and submitting forms), and their relatives, guardians and other persons associated with them
- businesses (including security companies, and other supplies of goods and services) and other private sector organisations working with the police in anti-crime strategies
- voluntary sector organisations
- local authorities, national and local government departments and agencies (including the Home Office, HM Revenue and Customs, and private safeguarding agencies)
- other law enforcement agencies and bodies (including international ones)
- partner agencies involved in crime and disorder strategies
- legal representatives, prosecuting authorities, courts, and prisons
- licensing authorities
- approved organisations and people working with the police
- ombudsmen and regulatory bodies (including the Independent Police Complaints Commission, and Her Majesty's Inspectorate of Constabulary)
- auditors
- Police and Crime Commissioners
- emergency services
- current, past or prospective employers of individuals
- healthcare, social and welfare advisers or practitioners
- education, training establishments and examining bodies
- business associates and other professional advisors
- our employees, agents, and other temporary and casual works
- persons making enquiries or complaints
- financial organisations and advisors, and credit reference agencies
- survey and research organisations
- trade, employer associations; and professional bodies
- individuals who contact us using social media applications, both publicly and privately.
- Information can be obtained from social media (such as Facebook, Instagram, YouTube, etc.) for the purposes of investigating criminal activity (manifestly made public by the data subject).
- the media
- our own CCTV systems and body worn cameras
- WhatsApp

What is our lawful basis for processing personal data?

Where we process personal data for the policing purpose our legal basis for processing is that it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us. Our functions and the official authority vested in us are set out, in the main, in the Police and Criminal Evidence Act 1984, the Police Act 1996, and the Police Reform Act 2002.

Where we process personal data relating to criminal convictions and offences, that processing is necessary for reasons of substantial public interest and involves the exercise of a function conferred on us by an enactment or rule of law. We have an appropriate policy document (as required under the Act) for that processing.

We will ensure that your personal information is handled fairly and lawfully with appropriate justification. We only use your information for lawful purposes.

Where we process personal data for purposes other than the policing purpose our legal basis for processing will vary depending on the circumstances. Ordinarily, the relevant legal basis is that the processing is:

- necessary for performing a contract
- necessary to comply with a legal obligation (including employment law)
- in the public interest or for official purposes
- necessary to protect your vital interests

and on occasion

- with your explicit consent (which you may withdraw at any time).

What security measures do we use when processing your personal data?

We take the security of all personal data under our control seriously. We comply with our legal obligations regarding security, relevant parts of the ISO27001 Information Security Standard, and where appropriate the College of Policing Authorised Professional Practice guidance on Information Assurance.

We ensure that appropriate policy, training, technical and procedural measures are in place, including audit and inspection, to protect our manual and electronic information systems from data loss and misuse. We only permit access when there is a legitimate reason and under strict guidelines on what use may be made of any personal data contained within them. We continuously manage and enhance our compliance with relevant standards and guidance to achieve adequate and up-to-date personal data security.

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.

What disclosures do we make of your personal data?

We may disclose personal data to a wide variety of recipients in any part of the world (including outside of the United Kingdom and the European Economic Area), including to those from whom we originally obtain personal data. Recipients may include:

- law enforcement agencies
- businesses (including security companies, and other supplies of goods and services) and other private sector organisations working with the police in anti-crime strategies)
- partner agencies working on crime reduction or safeguarding initiatives
- 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
- victim support service providers
- bodies or individuals working on our behalf
- authorities involved in offender management
- ombudsmen, auditors and regulatory authorities
- other bodies or individuals where required under any legislation, rule of law, or court order
- other bodies or individuals where necessary to prevent harm to individuals
- social media platforms for risk assessment purposes (consisting of addition of reference number(s) only)
- the media.

The Police decide disclosure on a case-by-case basis, ensuring only limited, necessary and proportionate personal information is shared under appropriate controls and safeguards. The Police are aware that references added to social media are visible to other members of the public using that site. However, please be assured that any enquiries in relation to these references is subject to stringent additional Data Protection screening to validate the identity of the caller.

Because of the way the website is set up, all completed online forms are automatically sent securely to the central police IT team responsible for delivery of the National Police Chiefs' Council Digital Policing Portfolio, as well as us.
If we make disclosures outside of the United Kingdom and the European Economic Area to locations which do not have as extensive data protection laws we ensure that there are appropriate safeguards in place to certify that the personal data disclosed is adequately protected.

How long do we retain your personal data?

We keep your personal data for as long as necessary for the particular purpose or purposes for which we hold it.
Police forces have a duty to obtain and use a wide variety of information (including personal information), in order to discharge their responsibilities effectively. They need the support and cooperation of the public in doing so.
If we place any of your personal data on the Police National Computer it will be retained, reviewed and deleted in accordance with agreed national retention periods, which are subject to periodic change.

We will retain records containing personal data relating to criminal investigations, intelligence, public protection, and custody in accordance with the College of Policing guidance on the Management of Police Information. Click here to read our retention policy.

What are your rights over your personal data we process, and how can you exercise them?

Under the Act you have a number of rights that you can exercise in relation to personal data we process about you. You do not have to pay to exercise your rights (other than a reasonable fee if a request for access is clearly unfounded or excessive but we agree to fulfil it anyway).

We sometimes need to request specific information from you to help us confirm your identity and ensure your authority to exercise the rights.

Right of Access: You can request access to the personal data we hold about you free of charge. Normally we will provide it within one month of receipt of your request unless an exemption applies. You can request access to the personal data we hold about you using the contact details in this privacy notice.

Right to be Informed: You are entitled to be told how we obtain your personal information and how we use, retain, and store it, and who we share it with. This privacy notice gives you that information, as well as telling you what your rights are under the relevant laws.

Right to Rectification: If we hold personal data about you that is inaccurate or incomplete you have the right to ask us to correct it. You can ask us to correct your personal data using the contact details in this privacy notice. We will reply to you within one month unless the request is complex.

Right to Request Erasure: Under certain circumstances you have the right to ask us to delete your personal data to prevent its continued processing where there is no justification for us to retain it. The circumstances most likely to apply are:

- where holding your personal data is no longer necessary in relation to the purpose for which we originally collected and processed it;
- where you withdraw your consent to us holding your personal data if we are relying on your consent to hold it.

The right of erasure does not apply if we are processing your personal data:

- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for the establishment, exercise or defence of legal claims
- to exercise the right of freedom of expression and information
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to make it impossible to carry out or seriously impair that processing.
- If you want to ask us to delete your personal data you can do so using the contact details in this privacy notice. We will respond to you within one month unless the request is complex.

Right to Restrict Processing: Under certain circumstances you have the right to ask us to restrict the processing of your personal data. This may be in cases where:

- you are contesting the accuracy your personal data while we are verifying the accuracy
- your information has been unlawfully processed and you oppose its erasure and have requested a restriction instead
- where we no longer require your personal data but you need it to establish, exercise or defend a legal claim and do not want us to delete it.
- You can ask us to restrict processing of your personal data using the contact details in this privacy notice.

Right to Data Portability: You have the right to obtain and reuse your personal information for your own purposes, transferring it from one environment to another. This right only applies to personal data provided by an individual, where the processing is based on their consent or for the performance of a contract and when that processing is carried out by automated means. If you wish to discuss this right, you can do so using the contact details in this privacy notice.

Right to Object: You have the right to object to under UK GDPR and not the Data Protection Act 2018.

- processing based on legitimate interests or performance of a task in the public interest and or exercise of official authority
- processing of your information for scientific and historical research and statistics
- direct marketing.

Any objection must be on grounds relating to your particular situation. If you want to exercise your right to object you can do so using the contact details in this privacy notice.

Rights related to automated decision making and profiling:

You have the right not to be subject to a decision when it is based on solely automated processing (including profiling) and which produces a legal effect or similar significant effect on you. This right does not apply if the decision is authorised by law, is necessary for entering into or performance of a contract or is based on your consent. We are unlikely to carry out automated decision making because our processes involve some type of human interaction and decision-making. Profiling is any form of automated processing of personal data intended to evaluate certain personal aspects about you to predict things about you such as your behaviour, interests, movements or performance at work. We do not currently carry out automated profiling. If you have any questions about automated decision-making or automated profiling, you can raise them using the contact details in this privacy notice.

Surrey Police and Sussex Police Public Website

We gather information about site usage to help the development and improvement of services to the public, and to protect the integrity of our systems from malicious users. We also gather information through the various functions available on the site that allow you to provide us with information (such as online forms and the live-chat function) for the purposes described later in this privacy notice. At the moment this information consists of:

- information obtained by our content management system to examine what people are searching for, what they find, and occasions where no results are returned, and which does not identify individual users; information provided by users through online forms (for purposes including crime reporting, crime reporting advice and information, anti-social behaviour reporting, 'Clare's Law' applications, road traffic incident reporting, and firearms licence applications) and live-chat functionality, which may identify individual users and other individuals depending on what information users enter. (it is possible we will be able to access information you enter on an online form even if you do not submit it, because of the way the website is set up to automatically save part-complete forms periodically).
- statistical information obtained using Google Analytics which does not identify individual users (more information about this is in the 'How do we use cookies?' section of this privacy notice)
- your IP address and details of which browser you are using, which we record when you use our online forms
- your IP address, used to identify your location if you use any geo-location features on this website, and which we only use to show you relevant content, and which we do not store or share with third parties.
- The Police utilise Civica payments as a portal to accept online payments for collision abstract reports. Civica are the Data Processor acting on behalf of the Police, their Privacy Notice can be found here. The Police are limited to the information they can view, which excludes customer financial details. Details provided through the portal will be retained under the HMRC guidance of 7 years, whereas card data will be kept for 2 years in line with PCI-DSS guidance.

How do we use cookies?

A 'cookie' is a piece of information stored on your computer which allows web servers to collect information from your visit to this website. It saves a small amount of data to your computer, which the website then uses on repeat visits.

We use cookies on this website to improve user experience and for essential functionality. We do not use them for identification, monitoring, or profiling purposes. To find out how to reject, delete or update your cookie preferences in your browser you need to know what browser you use and what version of it you are using. Most browsers have guidelines on how to adjust cookie settings through their 'Help' menu.

We use the following cookies on the website for the reasons explained below.

Google Analytics sets the following cookies:

Universal Analytics

Cookie name	Expiration time	Purpose
_ga	Two years	This cookie is used to distinguish users, which helps us count how many people visit our website
_gat	Ten minutes	Used to manage the rate at which page view requests are made

Google Analytics

Cookie name	Expiration time	Purpose
_utma	Two years	Like _ga, this lets us know if you've visited before, so we can count how many of our visitors are new to the site or to a certain page
_utmb	30 minutes	This works with _utmc to calculate the average length of time you spend on the site
_utmc	When you close the browser	This works with _utmb to calculate when you close your browser
_utmz	Six months	This tells us how you reached the site (eg from another website or a search engine)

If you don't want to send information to Google Analytics, you can use Google's opt-out browser add-on or you can configure your browser to enable you to choose which cookies you allow to be created.

'Remarketing' services
We use cookies from the Google Doubleclick and Facebook Pixel services to track activity of website visitors originating from media sources. We use anonymised data from this service to optimise our online advertising activity for recruitment. In certain cases we may use 'remarketing' services to target our ads to you based on your prior use of our site when you visit other sites included within an online advertising network. If you do not wish to be tracked in this way, you can opt out via the following:
Google Doubleclick

Facebook Pixel
- if you are a Facebook user
- if you are not a Facebook user

Session cookies
We use session cookies to enable us to identify requests from the same browser during a limited time window, and provide a way to remember page changes, or item or data selection, for the duration of that session.

Session cookies are essential for the website to operate and are set upon your arrival to the site. These cookies are deleted when you close your browser.

Site messages
You may see pop-up messages on our site. For example, a pop-up explaining our use of cookies. Once you have seen these messages, we store cookies to ensure we do not show you the same message again.

How you can complain

The Information Commissioner's Office (ICO) regulates the processing of personal data. You can complain to the ICO if you are unhappy with how we have processed your personal data.

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
Information Commissioner's Office website

Date of last update and changes

We last updated this privacy notice on 24/05/2022. We keep this privacy policy under regular review and update it if any of the information in it changes