



Privacy Notice: Surrey Police and Sussex Police

How we use Employment Data

Surrey Data Protection Officer: Kelly Thornton
dataprotection@surrey.police.uk
[Full Privacy Notice](#)

Sussex Data Protection Officer: Jim Collen
DPO@sussex.police.uk
[Full Privacy Notice](#)

The use and disclosure of your personal information is governed in the United Kingdom by UK Data Protection Legislation. The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (Law Enforcement purposes) 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.

Our Privacy Notice tells you how Surrey Police and Sussex Police hold, retain, process, disclose and share the information we obtain about you. It also explains the rights you have regarding your personal information.

The Chief Constables for Sussex police and Surrey police are defined as the '[Data Controllers](#)' for the purposes of the legislation and is 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.

What is personal information?

Personal data is any data that can be used to identify a living individual, on its own or in combination with other available information. References to names, identification numbers and location data are all personal data. Processing means anything we do with the data and includes collecting, storing and sharing.

Surrey Police and Sussex police collect and process personal data relating to people who work for us to manage the employment relationship from the point an individual expresses an interest in working for us, throughout employment and after employment has ended. This includes using information to enable us to comply with the employment contract, police regulations and other legal obligations as outlined in this Privacy Notice.

We will only use your personal information when the law allows us to and where it is necessary and proportionate to do so.

Information about you will be held in various formats including electronically in emails, in Surrey Police and Sussex Police People Management systems and in other Force managed IT systems, within your personnel file, as well as paper based records and on security systems such as CCTV and estate entrance mechanisms.

Most of the information we hold will have been provided by you directly, but some may come indirectly from other internal sources, such as your manager, or in some cases, external sources such as referees or members of the public.

We are committed to being transparent about how we collect and use that data to meet our data protection obligations.



What information do Surrey Police and Sussex Police collect about the people who work for us?

We collect and process a range of information about you. This includes:

- Your name, address and contact details, including email addresses and telephone numbers, data of birth and your gender;
- The terms and conditions of your employment including any variations to these;
- Details of your qualifications, skills, experience, training records, employment and postings history including start and end dates during your time working for us and those declared during your recruitment;
- Information about your remuneration, including entitlement to benefits such as pensions, insurance and health and wellbeing benefits;
- Deductions from your pay (voluntary and mandatory) including subscriptions such as sports and social, insurance, Unison and Federation subs etc.;
- Details of your bank account, taxation requirements and national insurance number;
- Information about your marital and partnership status, next of kin, dependants and emergency contacts;
- Information about your vetting status and integrity health check history including secondary business interests, associations, financial status and gifts declared;
- Details of your schedule including your working hours and shift patterns including shift allowances, flexible working requests and agreements, start, finish and break times, entrance and exit to police estate using your security pass and your attendance at work;
- Details of periods of leave taken by you (paid and unpaid) including holiday, sickness absence, family leave, study leave, career breaks, compassionate leave and leave for any other purpose including the reasons for the leave;
- Details of any disciplinary or grievance procedures in which you have been involved, including any sanctions (formal or informal) issued to you and related correspondence;
- Details of any complaints from the public which involve you including incidents involving death or serious injury. The Independent Office for Police Complaints (IOPC) investigate complaints from the public including those involving death or serious injury. During the complaint investigation process, personal data relating to the complaint or required by the investigation may be shared between ourselves and the IOPC.
- Assessments of your performance including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- Information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- Equal Opportunities monitoring information, including your ethnic origin, sexual orientation, religion or belief and health data;
- Details of the content and usage of Police IT and Communications equipment;
- Information that we are required to collect under Police Regulations (these apply to police officers only).
- Proof of your identity, such as a photocopy of your driving license;
- Photograph(s);
- CCTV footage and swipe card records;
- Health and Safety records;
- Secondary employment and volunteering;
- Correspondence with or about you;
- Legal documents relating to you;
- Records of any compensation claims and payments;
- Information about your use of our computer systems;

Surrey Police and Sussex Police collect this information in a variety of ways, for example through your application to work with us, your identification and vetting documents, forms such as the Diversity Monitoring form and communications with you including interviews, meetings, or other assessments.



In some instances the organisation collects personal data about you from third parties, such as employment references supplied by former employers, information from employment background check providers, information from credit reference agencies and from criminal records checks permitted by law.

All our third party service providers are required to take appropriate security measures to protect your personal information in line with our policies and data protection legislation. We do not allow our third party service providers to use your personal data for their own purposes. We will not:

- Sell your information to third parties
- Share your information with third parties for marketing purposes

Data is stored in a range of different places including within your personnel file, in Surrey and Sussex Police People Management Systems and in other Force managed IT systems including the email system.

Why do Surrey Police and Sussex Police process personal data?

If you are a member of police staff, we need to process personal data to enter into an employment contract with you and meet our obligations under that contract. If you are a police officer we need to process personal data to ensure we meet our statutory obligations under Police Regulations. For example we need to process data to pay you in accordance with our agreement with you and to administer benefits, pensions, expenses and allowances.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, we are required to check your entitlement to work in the UK, to deduct tax, to comply with health, safety and employment legislation and to enable you to take the leave you are entitled to.

In other cases the organisation has a legitimate interest in processing personal data before, during and after the end of an employment relationship. This allows us to:

- Run recruitment and promotion processes
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in an emergency) and records of our workforce contractual, regulatory and statutory rights
- Operate and keep a record of disciplinary, complaint and grievance processes to ensure that professional standards are maintained and there is acceptable conduct within the workplace
- Operate and keep a record of employee performance, skills and related processes, to plan for career development and for succession and workforce planning purposes
- Obtain Occupational Health advice, to ensure that we comply with duties in relation to individuals with disabilities, employment and health and safety law to ensure that employees are receiving the pay, benefits and fair treatment to which they are entitled;
- Operate and keep a record of leave including maternity, paternity, adoption, parental, shared parental and dependants' leave) to allow for effective workforce planning and ensure the organisation complies with duties in relation to leave entitlement and to ensure that you are receiving the pay or other benefits to which you are entitled;
- Ensure organisational change processes meet our legal and statutory obligations;
- Ensure effective and efficient general people management and business administration;
- Provide employment references for current or former workers;
- Understand and act on reasons for leaving through exit surveys and interviews
- Respond to and defend against legal claims;
- Publish information internally within Surrey Police and Sussex police relating to starters, movers and leavers so that the workforce are aware of workplace changes;
- Publish information internally within Surrey Police and Sussex police relating to gross misconduct outcomes relating to police officers as this is in the public interest;



- Publish information relating to suspension, arrest or charging for any criminal offence of any member of the workforce as this is in the public interest;
- Maintain and promote equality in the workplace;
- Promote effective communications within the organisation
- Undertake vetting processes upon you to ensure the integrity and security of our organisations and provide you with the security clearance appropriate for your role
- Ensure the security of staff, visitors, property and information. This includes preventing unauthorised access to and monitoring the use of our computer and electronic communications systems and preventing malicious software distribution
- Sharing business contact, duties and posting information

Where Surrey Police and Sussex Police rely on contract and legitimate interests as a reason for processing data, we have considered whether or not those interests are overridden by the rights and freedoms of our workforce and we have concluded that they are not.

Some special categories of personal data such as information about health and medical conditions is processed to carry out our employment law obligations (such as those in relation to people with disabilities, for health and safety purposes and to comply with the Employment Rights Act 1996).

In order to help you manage any issues that arise in connection with your health and wellbeing, to give the best professional support to you and your line manager and to meet our legal, statutory and contractual obligations, we collect, process and share (on a 'need to know' basis) information for example: reason(s) for absence, information on your fit notes and data you share with us relating to your medical condition(s) and treatment(s). We may obtain health data from third parties for example the Force Medical Officer (FMO) or from health Specialists appointed through Occupational Health with your consent.

We process special (UK GDPR) and sensitive (Data Protection Act 2018) categories of personal data such as information about ethnic origin, sexual orientation, religion or belief and this is done for the purposes of equal opportunities monitoring. Data that we use for these purposes is anonymised. You can ask us to stop processing this data at any time.

Surrey Police and Sussex Police aim to increase representation from under-represented groups to better reflect the communities we serve. In order to do this, we run positive action programmes to help and support people from under-represented groups during recruitment and promotion processes. We will seek your express consent to access this support which can be withdrawn at any time. You are entirely free to decide whether or not to provide the special data referred to above and there are no consequences for failing to do so.



Who has access to data?

Your information will be shared internally including with members of People Services (HR, Payroll, Finance, L&D and Recruitment), Professional Standards, your line manager, managers in the business area in which you work (who may be from Surrey Police or Sussex Police) and ICT staff if access to the data is necessary for their roles.

Some of your data is shared with external providers because they host the systems that provide certain services. These providers include:

- Occupational Health systems
- Recruitment system
- Expenses / budgetary forecasting systems
- Payroll provider
- National mutual aid system
- National police learning platform
- Leadership learning system
- National police promotions framework assessment
- Volunteers and specials system

In addition, data is shared externally with the following organisations as required:

- College of Policing (Police Constable Recruitment, Fast Track and National Police Promotion Framework assessment and approval, Barred and Advisory List)
- Pensions providers
- Government Departments such as HMRC and DWIP
- Benefit providers such as Lifestyle, Childcare Voucher administrators and Cycle to work schemes
- Sussex Police Charitable Trust (Sussex only – to provide benefits to members who wish to join)
- Surrey Police and Sussex Unison, Police Federation and Superintendents' Association – to provide benefits to members who wish to join
- External training providers
- Legal advisors

Professional Standards Department (PSD) will continually monitor Police records (including recruitment, People Services and Operational Policing records) throughout your employment in both Forces. This is to ensure the integrity and security of its workforce. This will include Domestic Abuse and other reported criminal activity involving serving officers and / or members of staff.

It is necessary and reasonable for the Police to identify these reports and address the safeguarding of serving officers and / or members of staff in order to manage the risk posed by them (especially if they hold a position of trust). This also allows for effective investigation and safeguarding for victims in circumstances where the position held by individuals could impact on the impartiality and independence of the police response.

In response to the Angiolini Report, this Privacy notices has been updated to ensure existing and prospective officers and staff are aware that they must be held to a higher standard of behaviour and accountability and that a right to privacy can be restricted in certain circumstances. These circumstances include, but are not limited to: recruitment, vetting, aftercare, transfer, promotion, role change, returning to policing and maintaining standards.

** Where you have provided your personal data to us for the purposes of the police constable recruitment process, your data, including biographical monitoring (diversity information obtained in accordance with the Equality Act 2010) 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.

Biometric (Fingerprints and DNA) information shared with Surrey Police or Sussex Police will not be shared with the College Of Policing. Further information can be found on the College of Policing [Privacy Notice](#).

We will not transfer your data to countries outside the European Economic Area.

How do Surrey Police and Sussex Police protect your data?

We take the security of your data seriously and we have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by employees in the performance of their duties. We share data only on a 'need to know' basis and ensure security in the following ways:

- Holding information sharing agreements with third parties with whom we share data
- Using the relevant Government Security Classifications (Official/Official-Sensitive) as appropriate
- Providing data handling instructions when sharing personal data
- Using secure email addresses to share data where possible
- Restricting ICT access to groups of users, password protecting or separating data access into groups of relevant users
- Providing training, advice, guidance and support to personnel relating to data sharing and the importance of privacy
- Protecting your information against unauthorised or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical and procedural measures

Where Surrey Police and Sussex Police engage a third party to process personal data on its behalf, they do so on the basis of written instructions and are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long do Surrey Police and Sussex Police keep your data?

We hold your data for the duration of your employment. After you leave the organisation, we adhere to the Retention Schedule. Please see the retention schedule on this page to view the specific retention periods for the data we collect and hold.

Your rights:

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request;
- Require us to change incorrect or incomplete data;
- Require us to delete or stop processing your data where the data is no longer necessary for the purposes of processing;
- Object to the processing of your data where the organisation is relying on its legitimate interests as the legal basis for processing;
- Ask the organisation to stop processing data for a period if there is a dispute about whether or not your interests override our legitimate grounds for processing data

If you would like to exercise any of these rights, please contact DataProtection@surrey.police.uk or information.governance@sussex.police.uk. If you believe that the organisation has not complied with your data protection rights, in the first instance please contact the Data Protection Officer.

You can also complain to the Information Commissioner <https://ico.org.uk/concerns/>



What if you do not provide personal data?

You have some obligations under your employment contract (or police regulations) to provide us with data. In particular you are required to report absences from work and may be required to provide information about disciplinary or other matters such as public complaints. You may have to provide us with data in order to exercise your statutory rights for example in relation to statutory leave entitlements or benefits available laid out in our policies. Failure to provide data may mean that you are unable to exercise your statutory rights or access benefits to which you are entitled.

Certain information such as contact details, your right to work in the UK, vetting information and payment details have to be provided to enable you to work in Surrey Police and Sussex Police. If you do not provide other information, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently and effectively.

Automated Decision Making

During recruitment, there are pre-selection criteria that must be met. If your answers indicate that you do not meet this, your application may be automatically rejected. During employment, decisions are not based solely on automated decision making.

Contact Us

If you have any concerns about how Surrey Police and Sussex Police has handled your personal information you should contact our Data Protection Officer by:

Email	Sussex	DPO@sussex.police.uk
	Surrey	dataprotection@surrey.police.uk

Address	Sussex	Data Protection Officer Sussex Police Headquarters Church Lane Lewes East Sussex BN7 2DZ	Surrey	Data Protection Officer Surrey Police PO Box 101 Surrey Guildford GU1 9PE

If you want to raise a concern with the Supervisory Authority

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 you may wish to contact them using the information below. Further information about the ICO can be found [here](https://ico.org.uk).

The Information Commissioner's Office,
Wycliffe House, Wilmslow, Cheshire, SK9 5AF
Telephone 0303 123 1113
Email casework@ico.org.uk

Changes to our Privacy Notice

We keep our privacy notice under regular review. This privacy notice was last updated on 21/05/2024.

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.