

# **Office of the Police and Crime Commissioner for Gwent Police**

## **Staff Privacy Notice**

### **Who we are**

The Office of the Police and Crime Commissioner for Gwent (OPCC) provides support to the Police and Crime Commissioner (PCC) in carrying out his duties and responsibilities which include holding the Chief Constable for Gwent to account for the delivery of local policing, setting and updating a police and crime plan, setting the budget and the precept and engaging with the public and communities within Gwent.

The Chief Executive of the OPCC is the data controller for the personal information we process, unless otherwise stated.

You can contact us in a number of ways

By email: [Commissioner@gwent.pnn.police.uk](mailto:Commissioner@gwent.pnn.police.uk)

By telephone: 01633 642200

By post: Office of the Police and Crime Commissioner for Gwent  
Police Headquarters  
Turnpike Road  
Croesyceiliog  
Cwmbran  
NP44 2XJ

The Data Protection Officer (DPO) is Joanne Regan. She can be contacted via the details above. Please mark all correspondence for the attention of the DPO.

### **Purpose of this privacy notice**

This privacy notice is to advise you of how your personal information will be dealt with (processed) by the OPCC and your rights in relation to that processing.

It is important to note that Gwent Police undertake all Human Resource and payroll functions on behalf of the OPCC and as such, your personal data will be shared between both organisations. Your personal data will be processed on behalf of the OPCC in the same way as that of a Gwent Police employee. 'We' and 'our' are used throughout this privacy notice, this should be taken as meaning the OPCC and/or Gwent Police. For further information on Gwent Police and their Data Protection Officer, please visit their [website](#).

## What information do we collect?

We collect a range of information about you. This can include:

- your name, address and contact details, including email address, telephone number, date of birth and gender;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, gender, disability and religion or belief;
- the terms and conditions of your employment;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your vetting and criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- photographs for your staff identification badge;
- details of periods of leave taken by you, including holiday, sickness absence, compassionate, emergency and dependant leave, career breaks, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- 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;
- details of trade union membership;
- welsh language (in line with Welsh Language Standards) and other language ability; and
- External business interests in line with our *business interests policy*.

We collect this information in a variety of ways. For example, data is collected through application forms, obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments. In some cases, we collect personal data about you from third parties, such as references supplied by former employers.

As part of your initial employment you will be required to undertake a vetting process. This requirement may be repeated periodically during your employment depending on your role. Any vetting checks we conduct will be in line with the College of Policing, Vetting Approved Professional Practice and depending on the vetting clearance level

required for your role we may ask you to provide your personal details as well as details of your partner, any children over the age of 10 years, your parents, siblings and co-residents.

Depending on the your role we may also carry out checks on criminal convictions, local intelligence, the Police National Database, open source checks and a credit reference agency checks. The level of vetting clearance required for each post will be determined in line with College of Policing Vetting Approved Professional Practice and the Vetting Code of Practice.

### **What is the legal basis for processing your personal data?**

We need to process your personal data to enter into an employment contract with you and to meet our obligations under this contract. For example, we need to process your data in order to provide you with an employment contract, to pay you in accordance with your employment contract or details of appointment and to administer pension entitlements, voluntary salary sacrifice schemes and deductions you choose to have made from your salary.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, we have a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure we comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that we comply with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general Human Resource and business administration;

- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where we rely on legitimate interests as a reason for processing data, we have considered whether or not those interests are overridden by the rights and freedoms of employees or workers and have concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow us to pay union subscriptions.

Where we process other special categories of personal data, such as information about ethnic origin, sexual orientation, gender, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

### **Sharing your personal data**

Your information will be shared internally, including with members of the Human Resource and Recruitment team, Payroll, your line manager, managers in the business area in which you work and SRS staff if access to the data is necessary for performance of their roles.

We share your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. We may also share your data with third parties in the context of TUPE of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

We also share your data with third parties that process data on our behalf in connection with pensions and the provision of benefits and the provision of occupational health services. Staff at South Wales Police who administer the Business World Human Resource and Payroll system with Gwent Police, will also have access to your data.

If your role requires wider government vetting we may provide your email address and other personal information such as your name, date of birth and passport number to United Kingdom Security Vetting (UKSV) who will contact you to complete the appropriate vetting application, UKSV will be the data controller for any additional information you provide to them.

We will not share your information with any third parties for the purposes of direct marketing.

## **How long do we keep your personal data?**

Personal Data is kept in line with our *retention policy*.

The organisation will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the National Police Chiefs' Council's National Guidance on the minimum standards for the Retention and Disposal of Police Records.

## **How do we keep your information secure?**

The OPCC takes the security of your data seriously. 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 its employees in the performance of their duties. Access to your personal data held on the Human Resource and Payroll system is limited to specific teams or individuals.

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

## **Your rights in relation to your personal data**

Under data protection law, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information.

- Your right of Access
- Your right to rectification
- Your right to erasure
- Your right to restriction of processing.
- Your right to object to processing
- Your right to data portability

Further information in relation to these rights can be found in our *general privacy notice*.

## **What if you do not provide personal data?**

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the

organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

### **Changes to this Privacy Notice**

We keep our privacy notice under regular review to make sure it is up to date and accurate.

### **If you are not satisfied**

We set very high standards for the collection and appropriate use of personal data and take any complaints very seriously. We would like you to bring to our attention any instance where you believe the use of data is unfair, misleading or inappropriate. We also welcome any suggestions for improvement. Please contact our Data Protection Officer for the OPCC in the first instance.

If you remain dissatisfied after contacting our Data Protection Officer, you can lodge a complaint with the Information Commissioner:

Information Commissioner's Office – Wales  
2nd Floor, Churchill House  
Churchill Way  
Cardiff  
CF10 2HH

Telephone: 01625 545297

Fax: 029 2067 8399

Email: [wales@ico.org.uk](mailto:wales@ico.org.uk)

**Updated 10<sup>th</sup> January 2019**