



Office of the
**Police and Crime
Commissioner**
for Warwickshire

Privacy Notice: Staff

Document Owner	Head of Business Services and Assurance
Version number	2
Policy Implementation Date	March 2024
Next Review Date Prior To	March 2026
Security Classification	Official
Disclosable under Freedom of Information Act?	Yes
Risk Rating	Medium
Equality Analysis	Medium

1. Introduction

The Office of the Police and Crime Commissioner (OPCC) is the data controller for any personal data held about you. The OPCC is committed to protecting your personal data. We are required under data protection legislation to notify you about how we manage your data and information, and this is explained in this privacy notice.

This notice applies to current and former employees, volunteers, workers and contractors. It also applies to the Chief Constable. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

OFFICIAL

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

2. Data protection principles

The OPCC will comply with data protection law, which means that your personal data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that have been clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes you have been told about and only limited to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes you have been told about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data from loss, misuse, unauthorised access and disclosure.

3. The personal information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Nationality.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.

OFFICIAL

- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race, gender and any disability.
- Information about your health, including any medical condition, health and sickness records.
- Where you leave employment and the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision.
- Details of any absences (other than holidays) from work including time on statutory parental leave and sick leave.
- Where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Information about criminal convictions and offences.

4. How we collect your personal information

We collect personal information about employees, workers, volunteers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

OFFICIAL

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

5. How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.
4. Where it is needed in the public interest or for official purposes (this will apply to the processing we carry out in connection with the appointment of the Chief Constable).

We may also use your personal information if we need to protect your interests (or someone else's interests), but this is likely to be rare.

The primary situations in which we will process your personal information are listed below. If you are a volunteer, not all of these situations will be applicable.

- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Providing benefits (as applicable).
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with the trustees or managers of your pension provider and any other provider of employee benefits.
- Administering the employment contract we have entered into with you.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.

OFFICIAL

- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.
- To publish anonymous equal opportunities statistics on our website.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

7. How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- a) In limited circumstances, with your explicit written consent.

OFFICIAL

- b) Where we need to carry out our legal obligations or exercise rights in connection with employment.
- c) Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment or there is another reason for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- Equal opportunities information on race, disability and gender is collected for anonymous publication on the OPCC website.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

8. Information about criminal convictions

All staff must pass police vetting before they begin work with us. The police vetting form has a separate Privacy Notice setting out how your personal data will be processed. Copies of completed vetting forms will only be retained by the OPCC for a specific reason, as generally applications are submitted through the online portal. We will keep a record of the outcome and date of the completed vetting; staff are required to notify of any changes to personal circumstances. Vetting renewals will be completed according to the Warwickshire Police policy.

9. Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you. We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

10. Sharing your personal data

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-parties process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents). The following third-party service providers process personal information about you for the following purposes:

- Warwickshire Police HR and Payroll team for the purpose of all HR and payroll services. Warwickshire Police will have access to all information that we hold about you (including health information) if required for HR and payroll purposes.
- Warwickshire Police Vetting Unit for the purpose of police vetting.
- The Home Secretary (in relation to the process of appointment of the Chief Constable only).
- The College of Policing (in relation to the process of appointment of the Chief Constable only).
- Warwickshire Police Pension administration for the purpose of providing the Local Government Pension Scheme.
- Benefit providers for the purpose of providing staff benefits (the list of benefit providers may change from time to time, but we can supply details on request)
- Warwickshire Police ICT services for the purpose of providing ICT services.
- Elected Technologies for the purpose of providing our case management system (but note that this software will only process staff names and not employment information).

We may also need to share your personal information with a regulator or to otherwise comply with the law.

How secure is my information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

11. Transferring information outside the UK

All data held within our case management system, Caseworker, is stored and processed electronically within Google's data centre in London, UK. However the software supplier, Elected Technologies, has a single third-party processor based outside the UK that they use for outbound transactional emails only. Elected Technologies have taken measures to ensure that the data is transferred in compliance with applicable law. The OPCC will not otherwise transfer your data outside the UK. However, if this is required at any time, any personal data transferred to countries or territories outside the UK will only be transferred in compliance with applicable law.

12. Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

13. Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention schedule. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we

OFFICIAL

process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, volunteer, worker or contractor of the OPCC we will retain and securely destroy your personal information in accordance with our data retention policy.

14. Your rights

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.
- If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your

OFFICIAL

other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

15. Data Protection Officer

The OPCC's Data Protection Officer is the Head of Business Services. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

16. Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

17. Revision Record

Date of change	Nature of revision
20 May 2021	General review of policy and update to include reference to case management software. Update to publication date. (DM)
March 2024	General Review and update to template (PR)