Employee Privacy Notice

Effective (Start) Date	**October 2019**
Last Review Date:	**September 2022**
Next Review Date Due:	**September 2023**
Business Area/Department	People Department
Contact/Author:	Michael Nulty – Compliance and Audit Officer Rachel Walsh – Data Protection Officer
Business Lead Approver:	Nicola Bailey – Head of People Services
Chief Officer Approval: ***(If appropriate see section 10)***	Julie Gill

1. Introduction

The General Data Protection Regulation (GDPR) requires Cheshire Constabulary to provide people with information about how it uses their information (a privacy notice). This privacy notice is relevant to all current, prospective and ex-'employees' (which includes staff, officers, specials and PCSOs). It also includes contractors, apprentices and volunteers who undertake roles similar to employees.

The Constabulary collects and processes a vast amount of employee personal data across multiple departments. We are committed to being transparent about how we collect and use that data. Therefore, this notice should also be read in conjunction with other Cheshire policies and procedures including the Records Management Procedure, Retention and Disposal of Records Procedure, along with the Full General Privacy Notice, DEI, PSD and vehicle telematics privacy notices.

In this notice, employees can be referred to as 'you' and Cheshire Constabulary can be referred to as 'we'.

2. Who "we" are

Cheshire Constabulary is a UK Police Force responsible for providing a policing function to the county of Cheshire. Our headquarters is based at Clemonds Hey, Oakmere Road, Winsford, Cheshire, CW7 2UA.

3. Why do we use your information?

We need to use and share your data to in order to fulfil our **contractual obligations** with you in relation to a contract of employment. For example:

- Running recruitment and promotion processes, including hiring temporary or permanent employees and provision of references.
- Monitoring and providing appropriate training (e.g., recruitment, promotion frameworks).
- Managing employee performance and related processes, planning for career development, succession planning and workforce management purposes.
- Maintaining accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), records relating to of employee contractual and statutory rights and records of absence in line with absence management procedures.
- Ensuring the integrity of new and existing employees, non-police personnel, contractors/suppliers. For example, vetting, investigations into allegations of misconduct, disciplinary or grievances by staff and PCSOs, alcohol or drugs testing.
- Recording Injury and near-miss data to support early retirement (ill-health pension).

- Allowing effective workforce management and operational management of buildings.
- Facilitating third-party payments as directed, to make payments to individuals and for finance to answer payment queries.
- Maintaining accurate and up-to-date pension records.

In some cases, we need to use or share your data to ensure that we are complying with **legal obligations**. For example:

- Undertaking health and safety risk assessments and any mandatory medicals, managing the process for accidents and near misses, along with the insurance claim process which can arise from these events.
- Maintaining and promoting equality, diversity and inclusion in the workplace, including enabling individuals to apply for promotion.
- Ensuring you are receiving pay or other benefits to which you are entitled.
- Deducting money owed to other organisations (e.g., student loan, court orders, tax code management, trade unions, pension provision).
- Allowing cardholders to purchase goods and services from a limited number of suppliers in the course of their duty.
- Investigating complaints/allegations of misconduct made internally or from members of the public and referring such matters to the IOPC where required.
- Preparing internal hearings concerning employee misconduct.
- Registering business interests, gifts and gratuities to monitor potential conflicts of interest and the likelihood of bribery.
- Maintaining key critical services in the event of an emergency.

Examples of law which provide a legal obligation

Health and Safety at Work etc. Act 1974, Driving at work regs 1997, The Management of Health and Safety at Work Regulations 1999, Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR), Pension Schemes Act 2021, The Local Government Pension Scheme (LGPS) Regulations 2014, Financial VAT Act 1994, Taxes Management Act 1970, National Insurance Contributions Act 2015, The Maternity and Parental Leave etc. Regulations 1999, Wages Act 1986, The Accounts & Audit Regs 2015, Money Laundering regulations, Employment Rights Act 1996, Employment Act 2008, Police (Promotions) Regulations 1996, The Police (Conduct) Regulations 2012, The Police Reform Act 2002, IOPC Statutory Guidance, The Police (Complaints and Misconduct) Regulations 2012, The Police (Conduct) Regulations, Code of Ethics, The Police Act 1996, The Equality Act 2010, Trade Union and Labour Relations (Consolidation) Act 1992, Civil Contingencies Act 2004.

Some of the information we use, and share is necessary for tasks that are in the **Public Interest.** For example:

- Running recruitment, promotion and exit processes which can include taking fingerprints, DNA and samples, officer vetting, support programmes such as positive action, exit interviews.
- Supporting health and wellbeing (e.g., preventing and managing sickness, appeals for medical redeployment, flexible retirement, obtaining medical

advice, ensuring employees are receiving the pay or other benefits to which they are entitled).

- Allowing effective workforce management such as for projects and programmes which improve operational effectiveness of the Force and supporting engagement with local people (e.g., publishing images of PCSOs/police officers in newspapers etc).
- Supporting the co-operation between employer, employees and trade unions. This can include successful delivery of service and the management of change.
- Ensuring system checks are carried out for a business/policing purpose and assets are tracked in compliance with regulations/codes.
- Investigating allegations of misconduct by Police Officers and Police Staff.
- Supporting the Cabinet Office's data matching exercise. The data matching allows potentially fraudulent claims and payments to be identified.

Examples of law which provide a Public Task

Employment Act 2008, Employment Rights Act 1996, ACAS Code of Practice, The Transfer of Undertakings (Protection of Employment) Regulations 2006 Trade Union and Labour Relations (Consolidation) Act 1992, Trade Union Act 2016, Vetting Code of Practice, Police Regulations, Special Constable Regulations, Police Reform & Social Responsibility Act 2011, The Police (Complaints and Misconduct) Regulations 2012, The Police Reform Act 2002, Health & Safety at Work Act 1979, The Equality Act 2010, Finance Act 2006, Immigration, Asylum and Nationality Act 2006, GDPR & Data Protection Act 2018.

In other cases, we have a **legitimate interest** to use or share your personal data. For example:

- Allowing individuals to register their interest to attend an event held by the Constabulary (e.g., recruitment webinars/promotion seminars) or be notified when recruitment opportunities arise.
- Running and organising sports and recreational groups as well as focus groups which are used to provide a collective view on topics of interest.
- Supporting employees by providing voluntary dyslexia screening tools.
- Publishing articles, videos and photographs internally which are written for the purpose of educating or informing members of the Constabulary about a topic, genre or an event.
- Facilitating internal communications (including surveys), collaboration on team projects and messages on approved platforms.
- Improving fleet utilisation/efficiency to ensure the operational effectiveness of the fleet.
- Allowing effective workforce management and operational management of buildings. This includes utilising CCTV for the safety and security of police personnel and premises.
- Responding to and defending legal claims.

Your information is not used for any marketing purposes.

Use of ‘Special’ data:

We may also need to use some information about you which is considered more sensitive. The GRPR calls this ‘special category’ data. Examples of such data include:

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data (where used for identification purposes), data concerning health, a person’s sex life and sexual orientation.

Some special categories of personal data are processed to carry out **employment law** obligations or in connecting with the **working capacity of the employee** (such as those in relation to employees with disabilities and for health and safety purposes). For example:

- Run an effective recruitment and promotion processes.
- To support health and wellbeing such as preventing and managing sickness, absence management, appeals for medical redeployment and flexible retirement.
- Where relevant in connection with a grievance or employee performance.
- Substance misuse testing.

Examples of law which support this:

Police Performance Regulations 2020, Police (Conduct) Regulations 2019 (Practice Requiring Improvement (PRI) and the Reflective Practice Review Process (RPRP)), Code of Ethics for Policing, Home Office Guidance (Performance and Attendance Proceedings), Employment Rights Act 1996, The Employment Tribunals (Constitution and Rules of Procedure) Regulations 2013, Health and Safety at Work Act 1974.

Some special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, is used in the substantial public interest for the purposes of **monitoring equality of opportunity**. This is undertaken in accordance with The Equality Act 2010 and includes monitoring race and ethnic diversity at senior levels.

Moreover, the special categories of personal data may also be required in line with **statutory and government purposes**. Please refer to the ‘public interest’ and ‘legal obligations’ listed above for more details on what these purposes are.

Sometimes, we use your special data when you have **made the information public.** Examples include:

- During the organisation and running of sports and recreational groups as well as focus groups which are used to provide a collective view on topics of interest.
- When you wish to share a personal experience or story to help others gain an insight on the topic. These are usually shared via our communications department.

In some instances, we will seek your **consent** to use or share your special data. Where we do this, you have additional rights such as changing your mind, asking us to stop using this data and asking us to delete it. Examples of the instances where we ask for your consent are:

- To disclose information to your line manager or psychologist (where relevant) as part of the dyslexia screening process.
- To publish articles which contain special category data which written for the purpose of educating or informing members of the Constabulary about a topic, genre or an event.

Note: sometimes the word 'consent' can be used during your employment, but it does not have the same meaning and rights as a GDPR lawful basis. Usually, this is a requirement supported by law and means you cannot withdraw or have genuine choice or control over the matter. An example where this applies is:

- When we obtain fingerprints and DNA samples to allow for a speculative search to be made against the local and national databases.

These instances are supported by law which gives us a legal obligation or a public task. We will tell you when the law requires us to obtain this type of data.

Use of criminal data:

Criminal information and special data (where relevant) will be used during your employment with us in order to **protect the public against dishonesty.** This can include escalating its use for a **law enforcement purpose.** For example:

- Ensuring the integrity of new and existing employees.
- Investigating complaints made internally or from members of the public.
- Pursing criminal investigations where a criminal offence is evident.

4. What information do we collect about you?

We can collect and process a wide range of information about you to support the purposes identified above. This may include:

- Basic identifiers such as your name, date of birth, gender, address and contact details.
- Information about your marital status, next of kin, dependants and emergency contacts.
- Financial details such as your bank account, payroll number, national insurance number, remuneration, including entitlement to benefits such as pensions or insurance cover and trade union membership.
- The terms and conditions of your employment, including details of qualifications, skills, experience, employment history, references, start and end dates with previous employers and your ability to drive.
- Information about your nationality, entitlement to work in the UK, criminal record and political affiliation. IP address and social media details can also be required.

- Certain roles within the organisation require biometric vetting (fingerprints and DNA), drug screening, medical tests and ongoing fitness to work assessments.
- Information about medical or health conditions, including whether or not you have a disability for which the organisation may need to make reasonable adjustments or monitor the equality of opportunity.
- Details of your schedule (days of work and working hours), attendance at work, details relating to periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals.
- Assessments of your performance, including appraisals (Performance Conversations), training you have participated in, performance improvement plans and related correspondence.
- Driving behaviours (example harsh braking, idling, blue light running, speed etc) via vehicle telematics software.
- location data (e.g., via Airwave radios at the time of making the transmission and via vehicle telematics).
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- Photographs and videos (e.g., the purposes of security, communications and engagement, including photographs of tattoos and injuries where required and significant).

Who can give us this information?

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; 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, the organisation collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

5. Who has access to your information?

Your information will only be shared when it is necessary to do so. Any information shared will be minimal to the purpose of the sharing. Any information shared will be done so via secure means.

Your information can be shared internally, including with members of HR, Finance, Estates and Fleet. It may also be necessary to share your information with your line manager and managers in the business area in which you work. For example, this

may be necessary to resolve a performance at work issue. It may also be necessary for IT staff to access your data in order to resolve any technical issues.

It is of paramount importance to preserve the integrity of the police service in order to ensure continued public trust. In order to preserve this integrity, it may be necessary to share your information with departments such as Professional Standards or even other forces.

Your data may also be shared with employee representatives (e.g., Unison and Federation) in the context of collective consultation on a redundancy or business sale. This would be limited to the information needed for the purposes of consultation, such as your name, role and length of service.

We can also share your data with third party organisations such as your previous employer, providers who provide payroll, pensions, benefits, testing, educational services, occupational health or support provision.

We can also share your data with third parties where there is a legal requirement such as legal representatives, courts, ombudsman, HMRC, home office, Health & Safety executive and DWP.

It is unlikely that your data will be transferred to countries outside the European Economic Area (EEA) but where it is, it will be done in accordance with the GDPR.

6. How do we protect your data?

We have multiple controls in place to ensure your data is handled securely and minimise the risk of your data is being lost, misused, disclosed in error or accidentally destroyed. Examples of controls include:

Having an information assurance regime in place to oversee the effective and secure processing of your personal data. More information on this framework can be found on our website.

Ensuring any third parties who process personal data on our behalf are given written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of your data.

Having strict procedures in place in the event that your data is lost, accidentally destroyed, misused or disclosed. In the unlikely event that this happens, and you are at risk of harm you will be contacted as soon as possible.

7. How long do we keep your data?

Each department will retain your personal data for as long as is necessary for their purpose(s). Some specific periods are outlined in the National Police Chiefs Council (NPCC) National Guidance on the Minimum Standards for the Retention and Disposal

of Police Records. Any exceptions to this will be as a result of an agreed requirement to retain certain information outside of the NPCC minimum requirements. These can be found on our general privacy notice.

8. Is your data subject to automated decision making or profiling?

Your data is not routinely subject to solely automated decisions that will have a significant impact on you unless we have a lawful basis for doing so. We do apply an automated decision to our E-Recruitment System when filtering out those who do not meet eligibility criteria to work in the UK. These criteria have been written in accordance with legislation, such as the Asylum and Immigration Act 1996. If do not agree with the outcome following an automated decision, you have the right to ask for this to be reviewed by a human. Please see Section 9 for more detail.

9. What are your rights?

You have the right under Data Protection legislation to request a copy of your information (subject to exemptions). For example, to know what it is used for and how it has been shared. This is called the right of subject access.

In addition to the right of access, you also have other rights, such as;

- the right to have inaccurate information rectified.
- to ask for information to be erased where consent is withdrawn or where other grounds apply.
- to have your information restricted (subject to conditions).
- the right to have your data transferred to another organisation (data portability) where the lawful reason for us using your data is based on consent or contract and it is carried out by automated means.
- the right to object where the lawful reason for us using your data is based on legitimate interests or a task in the public interest, including profiling.

For detail of how to make such a request, please visit the Privacy Notice page on our website: cheshire.police.uk.

You also have rights where a decision is made about you which can produce significant or legal effects and is made by solely automated means. Within one month of the decision taking place, you have the right to express your point of view and to contest the decision. In these instances, a human will consider the decision made.

10. The Data Protection Officer

You have the right to contact the Data Protection officer if you have any concerns about the way the organisation uses your data. They can be contacted via emailing requests@cheshire.police.uk, telephoning 01606 362384 or writing to:

Data Protection Officer, Cheshire Constabulary Headquarters, Clemonds Hey Oakmere Road, Winsford, Cheshire, CW7 2UA.

11. Making a complaint about your personal data

If you have a complaint about the way in which your personal data has been processed, you should contact the Data Protection Officer (details above) in the first instance.

If you are dissatisfied with their resolution to your complaint, you also have the right to complain to the Information Commissioner's Office who can be contact at the following address:

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

They can also be contacted by telephoning 08456 306060 or 01625 545745 or by visiting their website at www.ico.org.uk.