Cheshire Constabulary

Employee Privacy Notice

Effective (Start) Date	**October 2019**
Last Review Date:	**April 2021**
Next Review Date Due:	**April 2022**
This Procedure is suitable for publication under the Freedom of Information Act	**Yes** *(Delete as appropriate refer to FOI Section 6)*
Business Area/Department	People Department
Policy Contact/Author:	Michael Nulty – Compliance and Audit Officer
Business Lead Approver:	Nicola Bailey
Chief Officer Approval: *(If appropriate see section 10)*	Julie Gill

Cheshire Constabulary collects and processes personal data relating to its employees to manage the employment relationship. It is committed to being transparent about how it collects and uses that data.

The General Data Protection Regulations (GDPR) requires the Constabulary to provide you with information about how we use your information. This has been done in the form of this privacy notice which is relevant to all employees, prospective employees, including contractors, apprentices and volunteers. This privacy notice should be read in conjunction with other Cheshire information policies and procedures including the Records Management Procedure, Retention and Disposal of Records Procedure and Full Privacy Notice.

In this notice, employees are referred to as 'you' and Cheshire Constabulary is referred to as the 'organisation'.

1. Who "we" are

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

Multi Force Shared Service is a shared service hosted by Cheshire Constabulary who provide administrative support in a number of areas including HR, Accounts and Payroll. As part of the services MFSS provide they have access to create and amend your data. All data is held on the organisation's IT infrastructure and therefore apply the organisation's data security controls.

2. What information do we collect about you?

The organisation collects and processes a range of information about you for the process of managing recruitment, employment, remuneration and work related to your role within the organisation. Dependent on your role this may include:

- Your name, address and contact details including email address and telephone number, age, date of birth and gender;
- The terms and conditions of your employment;
- Details of your qualifications, skills, experience and employment history, including references, start and end dates with previous employers and with the organisation and your ability to drive;
- 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 marital status, next of kin, dependants and emergency contacts;
- Information about your nationality and entitlement to work in the UK;
- Information about your criminal record;
- Details of your schedule (days of work and working hours) and attendance at work;

- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- The outcome of medical tests used for the purposes of recruitment and ongoing fitness to work assessments;
- Biometric vetting (fingerprints and DNA) and drug screening information needed for the purpose of certain roles within the organisation.
- Photographs for the purposes of security, communications and engagement, including photographs of tattoos where required and significant.
- 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 Conversations), 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 and political affiliation; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

3. How do we collect 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.

4. Why do we need your information?

The organisation needs to process your data to in order to fulfil its **contractual obligations** with you in relation to your employment. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its **legal obligations**. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws, to enable employees to take periods of leave to which they are entitled, and to consult with employee representatives if redundancies are proposed or a business transfer is to take place. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the organisation has 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, and 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 that it complies with duties in relation to individuals with disabilities, meet its 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 the organisation complies 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 HR and business administration;
- Conduct employee engagement surveys;
- Provide references on request for current or former employees;
- Respond to and defend against legal claims; and
- Maintain and promote equality in the workplace.
- Information about trade union membership is processed to allow the organisation to operate union subscriptions.

Some of the information we process is necessary for tasks that are in the **Public Interest.** For example, we may publish public-facing roles or senior management roles to raise awareness of those role within the community. We also ensure that the public are protected from dishonesty by declining any individual whose criminal history is deemed sufficiently serious.

Where the organisation relies on its **legitimate interests** as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not. Where you feel that your interests not to have your information processed outweigh those of the organisation you have the right to object. If you wish to object to the organisation processing this data please write to the Data Protection Officer (see section 10).

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).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is

done in the substantial public interest for the purposes of equal opportunities monitoring.

Where personal data is needed to be acquired or shared with a third party the organisation will ensure a GDPR lawful basis permits the sharing. In some instances, this will involve us seeking your consent.

Where consent is requested, you have additional rights such as you can ask us to stop processing this data at any time by contacting the Data Protection Officer (see section 10)

Your information will not be used for any marketing purposes.

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 will be shared internally, including with members of the HR and the recruitment team (including payroll via the Multi Force Shared Service). 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.

Your data may also be shared with employee representatives 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.

The organisation shares your data with third party organisations, such as your previous employer, in order to obtain pre-employment references and to complete employment background checks. This can also include sharing your data, where relevant, with organisations which provide testing and educational services.

The organisation also shares your data with third parties that process data on its behalf, in connection with payroll, pension, the provision of benefits and the provision of occupational health services.

Your data may be transferred to countries outside the European Economic Area (EEA) for policing purposes. Any personal data transferred outside the EEA will be done so in accordance with the GDPR.

6. How do we protect your data?

The organisation is required to ensure that your data is handled securely. The organisation has multiple controls in place to minimise the risk of your data is being lost, misused, disclosed in error or accidentally destroyed.

The organisation has 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.

We have a Data Protection 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.

Where the organisation engages third parties to process personal data on its 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.

7. How long do we keep your data?

The organisation will retain your personal data for as long as is necessary which will usually be for the duration of your employment. The specific periods we keep your data for is 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 the organisation's intranet pages.

8. Is my 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 and we have notified you. Examples where we use automated decisions include;

- Our E-Recruitment System allows for automated decision-making to be used to check eligibility criteria for certain vacancies. These criteria have been written in accordance with legislation, such as the Asylum and Immigration Act 1996.

- Automated decision-making via scoring may be used should you undertake any assessment with a third-party company for Recruitment or Promotion processes. This is necessary or entering into, or performance of, a contract between you and the organisation.

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; and
- 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.pnn.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.