Cheshire Police and Crime Commissioner Privacy Statement on GDPR

Introduction

1. The General Data Protection Regulations (GDPR) came into force in May 2018, and brought into force new rules about how organisations can handle personal data.
2. This statement sets out what personal data the PCC holds, our purposes for processing that data, the lawful basis we have for doing so, who we share that information with, your individual rights in relation to that data, and some ancillary information about data security, data retention (how long we hold the data) and data breaches.
3. This document is intended to serve as a 'privacy statement' within the requirements of the GDPR to explain how we handle personal data.

Business Purpose for Processing Data

4. We have the following key business purposes for processing personal data:

   i. The effective personnel management i.e. PCC staff, volunteers and contractors as well as recruitment functions. Note that this is contained in a separate Employee Privacy Notice and so is not considered further in this privacy statement.

   ii. To engage with our partner organisations and contracted service providers to progress joint policing, criminal justice, victim support and community safety objectives and related matters. Our partner organisations include national and local public, private and voluntary organisations and an indicative list of these organisations is set out at Annex A for information.

   iii. To assist members of the public who have contacted us for help or advice about specific issues or who have raised complaints.

   iv. To effectively administer Committees and Panels and communicate with Committee and Panel members.

The 'Business Related' personal data we hold

Partner Organisations and Contracted Service Providers

5. We hold business email and postal addresses, and business telephone numbers. Annex A (below) sets out an indicative list of our stakeholders / partner organisations.

Members of the public

6. We hold information they have supplied to us, to enable us to respond to them. This may include home or business addresses, personal and/or business email addresses and personal or business phone numbers. This may include some “Special Category” data, as defined below – but only where the member of the public has offered this information to us of their own volition.

Committee and Panel Members

7. We hold home and/or business email and postal addresses, and telephone numbers, together with information required to assess potential conflicts of interest and to be able to pay expenses. This may include some “Special Category” data.

Lawful Basis for Processing Personal Data

8. The legal basis for our use of information will vary depending on the particular circumstance. These are some examples:

- Contract: The use of personal information could be necessary for the performance of a contract.

- Public task: The use of personal information could be necessary for the performance of public interest tasks e.g. working with partner organisations, responding to public concerns.

- Legal obligation: The use of personal information could be necessary for compliance with a legal obligation e.g. complaints procedure, use of ethnicity data to comply with Equality legislation.

- Consent: If you give your consent then we can process your personal information for that particular purpose.

"Special Category" Personal Data

9. The GDPR contains specific requirements about the handling of “Special Category Data”. This is personal data which is regarded as particularly sensitive and includes race, ethnic origin, politics, religion, health, sexual orientation, genetic information, etc.
10. In order to process special category information, organisations must satisfy a specific condition (from a limited range set out in Article 9(2) of the GDPR). The following applies:

- The public – The information provided to us by members of the public may include some “Special Category” data – but only where the member of the public has offered this information to us of their own volition.

Sharing Personal Information

11. Personal data belonging to members of partner organisations – Where we hold personal data, we do not generally share this without the permission of the data subject, except in exceptional circumstances i.e. there is an urgent need that a third party is able to contact that person.
12. Personal information from members of the public – unless there is a compelling public interest in doing so (i.e. to protect your safety or that of other people), we do not share this data without first seeking the agreement of the member of the public.
13. Personal data belonging to Committee and Panel members – Where we hold personal data, we do not generally share this without the permission of the data subject, except in exceptional circumstances i.e. there is an urgent need that a third party is able to contact that person.
14. We will not transfer personal data to countries outside the EEA.

Your Rights

15. The GDPR protects the rights of individuals about how personal information is held. Individuals have the following rights (except in certain specific circumstances):

    i. *The right to be informed about the collection and use of your personal data* - This means we must explain our purposes for processing your personal data, our retention periods for that personal data, and who it will be shared with. That is what this document aims to do.

    ii. *The right of access* – this allows you the right to be aware of the personal data and any supplementary information we hold about you and allows you to check that our processing is lawful. However, we must verify your identity before allowing you access.
    iii. *The right to rectification* – you have the right to ask us to correct your personal data where it is inaccurate or incomplete. You can make this request either verbally or in writing and we must respond within one month. We do not have to make a change if we think the data is accurate or if we believe the request is manifestly unfounded or excessive.

    iii. *The right to erasure* – you can ask us to erase your personal data (also known as the 'right to be forgotten'). The section below on Our Data Protection Policy sets out information about how long we would normally retain data before erasing it, but if you want us to erase personal data before the end of that period, you can ask us to do so, either in writing or verbally. We will respond within one month, and we can only refuse to erase personal data in a limited number of circumstances which are set out in the ICO guidance

    iv. *The right to restrict processing* – you can ask us not to share your personal data (as set out in the section on Sharing Personal Information), under specific circumstances if you have contested the accuracy of the data or our lawful basis for processing it.

You can also ask us to hold your data but not share it, where we would normally delete under our retention policy, but you need us to keep it in order to establish, exercise or defend a legal claim.

v. *The right to data portability* – this right only applies where the lawful basis for processing is consent or for the carrying out of a contract, and processing is carried out by automated means. These conditions do not apply to the PCC or the personal data we hold.

vii. *The right to object* – you have the right to object to our processing of your personal data. We must comply with your request unless we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms.

viii. *Rights in relation to automated decision making and profiling* – the PCC does not use these.

Data Retention Policy

16. This sets out a summary about how long we retain different types of personal data before we delete it. This varies according to the type of personal data it is:

- **Partner Organisations** – we retain personal details until we are informed that the individual concerned has left their post in that organisation.

- **Members of the Public** – We will retain members of the public personal data for 3 years from the date you contact us, or three years from the date we last provided advice or help to resolve your issue, where appropriate, unless we are asked to destroy it earlier or are asked to retain it longer by the data subject.

- **Committee and Panel Members -** we retain personal details for 6 months after the date we are informed that the individual concerned has left their post.

Information audit

17. We have undertaken an internal audit to identify the types of personal information we hold. This is set out in 'The 'Business Related" Personal Data We Hold' section of this policy.

Security measures

18. We take the security of business-related personal data seriously. We have controls in place to protect personal data against loss, accidental destruction, misuse or disclosure

and to ensure that data is not accessed, except by employees in the proper performance of their duties. We:

- Keep paper-based files containing personal information in locked drawers in a secure office.

- The Commissioner's Office takes the security of all personal data under our control very seriously. We comply with the relevant parts of the Data Protection Act 2018 relating to security and relevant parts of the ISO27001 Information Security Standard.

  We will ensure that appropriate policy, training, technical and procedural measures are in place, including audit and inspection, to protect our manual and electronic information systems from data loss and misuse. We will only permit access to them when there is a legitimate reason to do so, and then under strict guidelines as to what the personal data can be used for. These procedures are continuously managed and enhanced to ensure up-to-date security.

- Will ensure that all applicants for OPCC Jobs are advised of our data retention policy as part of our application pack.

19. OPCC Employees who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes. Not to disclose data except to individuals (whether inside or outside the OPCC) who have appropriate authorisation.

- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection and secure file storage and destruction).

- Not to remove personal data, or devices containing or that can be used to access personal data, from the OPCC's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

- Not to store personal data on local drives or on personal devices that are used for work purposes.

- To take care to ensure that PC screens and terminals are not visible except to authorised OPCC employees.

- To take care that manual records:

  - Are not left where they can be accessed by unauthorised personnel.

  - Are destroyed using secure methods as soon as they are no longer required.

  - To report data breaches of which they become aware to our Data Protection Officer immediately.

Data Breaches

20. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If a breach does occur, we must inform the Information Commissioner within 72 hours. We must also notify you as soon as possible if the breach carries a high risk to your rights and freedoms. In the unlikely event that this occurs, we will discuss with you how best to address any adverse consequences that might arise from the breach.

Our Data Protection Officer

21. We have appointed a Data Protection Officer (DPO) to help monitor our compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits. If you have any concerns about your data or how we process it, you should contact the DPO in the first instance using the details set out below (under Contact, Complaints and Concerns).

Contact, Complaints or Concerns

22. If you have concerns or queries about how we handle your data, you should contact our Data Protection Officer:

    Matt Walton – Senior Governance and Performance Officer
    Phone: 01606 364000
    Email: police.crime.commissioner@cheshire.pnn.police.uk

23. If you are not satisfied with how we have handled your query or the action we have taken as a result, you can:

- Contact the OPCC Chief of Staff at peter.astley@cheshire.pnn.police.uk
- Contact the Information Commissioner

24. In some circumstances, you might also be able to enforce your rights through legal action/the courts. You may want to seek independent legal advice about this, where appropriate.

25. The Police and Crime Commissioner for Cheshire and Cheshire Constabulary may use a range of methods, including face-to-face interviews, telephone and postal surveys, both to identify community priorities and to establish public satisfaction levels so our performance and effectiveness can be evaluated and improved. Depending on the purpose of the survey, the questionnaires may be targeted at members of the public chosen randomly according to accepted statistical principles, or specifically at victims or witnesses of crime or other incidents. Like many

organisations we may use a private company to undertake some surveys on our behalf with strict controls to protect the personal data of those involved.

Annex A

Indicative List of our Partner Organisations

The following is an indicative list of the main partner organisations where we hold the business email and postal addresses and business telephone number of some staff and officers:

- Cheshire Constabulary
- Cheshire West and Chester Council
- Cheshire East Council
- Warrington Council
- Halton Council
- Cheshire and Greater Manchester CRC
- Other Police Forces
- National and Local Media Organisations
- NHS Trusts and other health providers
- Association of Police & Crime Commissioners
- Crown Prosecution Service
- HM Courts and Tribunal Service
- HM Prison and Probation Service
- Legal Aid Agency
- Voluntary Organisations, such as Citizen Advice Bureau, Remedi UK, Leaders Unlocked