Derbyshire Police and Crime Commissioner
Safer and Stronger Together
Protecting Communities Fighting Crime

Office of the Police and Crime Commissioner for Derbyshire

Privacy Notice

EXTERNAL

Control Sheet

Policy details

Policy Title	OPCC Derbyshire Privacy Notice
Responsible Officer	Head of Compliance
Security Classification	OFFICIAL
Disclosable under FOIA	Yes
Policy implementation date	September 2026
Next review date	September 2028

Revision details

Revision date	**Changes**
November 2025	Review of the policy content – MR.
September 2026	Reviewed policy and added BCRP details – MR.

Contents

Topic	Page
1)Introduction	Page 4
2) Who we are	Page 4
3) The Data Protection Principles	Page 5
4) Lawful basis for processing	Page 6
5) What personal data do we process	Page 6
6) Special Category Data	Page 7
7) What do we use the personal data for	Page 7
8) Whose personal data do we handle	Page 8
9) Method of collecting personal data	Page 8
10) Who do we share personal data with	Page 9
11) Processing Activities • General correspondence (Inc. complaints against the CC, the PCC, the Deputy PCC and OPCC staff inc. Complaint Reviews, Anti-Social Behaviour Case Reviews (ASBCR), misconduct proceedings and Police Appeal Tribunals (PAT)	Page 10
• Grants and commissioned services	Page 13
• Business Crime Reduction Partnership	Page 15
• Holding to account	Page 17
• Subject access and FOI requests	Page 20
• OPCC managed websites and Social Media Channels.	Page 21
• Media enquiries	Page 23
• Public Consultations, Focus Groups and Event Booking Forms	Page 24
• Photographs and filming	Page 26
• Visiting the office	Page 27
• Applying for a job or volunteer role	Page 29
12) Failure to provide personal data	Page 31
13) Sharing your personal data	Page 31
14) How long is personal data retained?	Page 32
15) You Individual Rights	Page 32
• Right to be Informed	Page 32
• Right of Access	Page 33
• Right to Rectification	Page 34
• Right to Erasure/to be Forgotten	Page 34
• Right to Restrict	Page 36
• Right to Data Portability	Page 37
• Right to Object	Page 37
• Rights relating to Automated Decision Making	Page 38

16) Restrictions on Data Rights	**Page 39**
17) Right to withdraw Consent	**Page 40**
18) Data Protection Officer/OPCC contact details	**Page 40**
19) Right to lodge a complaint with the ICO	**Page 40**
20) Transfers of personal data abroad	**Page 41**
21) Further processing	**Page 41**
22) Automated decision making and Profiling	**Page 41**
23) Children's personal data	**Page 41**
24) Service adjustments/Equalities Act 2010	**Page 41**
25) Restricted contact	**Page 43**
26) Single point of contact	**Page 42**
27) How we keep your personal data safe	**Page 43**
28) Changes to this notice	**Page 44**

1) Introduction

1.1 Your privacy is very important to us and our Privacy Notice attached has been written in accordance with the relevant data protection laws.

1.2 Our Privacy Notice has been written to tell you what personal data the Office of the Police and Crime Commissioner (OPCC) for Derbyshire will process and why. 'Processing' includes how we –

- collect personal data,
- why we collect data,
- who we share the data with,
- how long we retain the data for, and how we dispose of it.

This notice also provides you with details of the rights you have in regard to any personal data we hold about you now and any personal data we might collect about you in the future.

1.3 In accordance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), a Data Protection Officer has been employed by the OPCC to help ensure that the personal data we hold is processed in accordance with the requirements, Regulations and Laws. The Data Protection Officer is also available to provide you with advice and assistance if you have any queries or concerns about how we process your personal data, their contact details can be found near the end of this notice.

2) Who we are

2.1 The Police and Crime Commissioner (PCC) is a public authority, established in legislation through the Police Reform and Social Responsibility Act 2011. For the purposes of this privacy notice, the term 'PCC' is used to encompass the person elected as the PCC, and any staff authorised to work for, or on their behalf, or under their direction and control of the OPCC.

2.2 The OPCC is the data controller for any personal data the organisation holds about you. The OPCC respects your privacy and is committed to protecting your personal data. A description of the personal data the OPCC processes, including how and why we process your personal data, who we share it with, and your rights and choices when it comes to your personal data is set out in this document.

2.3 The PCC obtains, holds, uses and discloses personal data for two broad purposes:

1. To discharge the remit, powers and duties of the PCC including rendering assistance to the public in accordance with PCC policies and procedures; and any duty or responsibility of the PCC arising from common law or statute.

2. The provision of services to support the remit of the PCC - including:

- Management of public engagement and communications, media relations, social media, advertising and website maintenance
- Financial management, accounts and administration, issuing grants
- Internal audit functions
- OPCC staff recruitment, training and development, staff administration, occupational health and welfare.
- Misconduct, Police Appeal Tribunals, pension forfeitures
- Management of complaints and queries from members of the public, appeals, reviews, data requests
- Management of OPCC data technology systems
- PCC's Volunteering Schemes
- Business Crime Reduction Partnership functions
- Police and Crime Panel functions
- Provision of support and administration to committees and panels that serve the PCC and CC to discharge their respective statutory responsibilities
- Certain manual files linked to the previous Police Authority

3) The Data Protection Principles

3.1 The OPCC will comply with all relevant data protection laws (The UK General Data Protection Regulations (UKGDPR), and The Data Protection Act 2018 (DPA2018). The UK GDPR outlines seven key data protection principles that must be followed by organisations when processing personal data.

These principles are:

- **Lawfulness, Fairness and Transparency**
  Personal data must be processed in a lawfully, fairly and transparent way.

- **Purpose Limitation**
  Personal data must be collected for specified, explicit and legitimate reasons and must not be further processed in a manner that is incompatible with those purposes.

- **Data Minimisation**
  Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

- **Accuracy**
  Personal data must be accurate and where necessary kept up to date.

- **Storage Limitation**
  Personal data must be kept only as long as necessary for the purpose/s of the processing.

- **Integrity and Confidentiality**
  Personal data must be kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect the personal data from loss, misuse, unauthorised access and disclosure.

- **Accountability**
  The OPCC are responsible for demonstrating compliance with all the UK GDPR principles. This includes having appropriate policies, procedures, and documentation in place to show how we are meeting our data protection obligations.

4) Lawful basis for processing

4.1 The OPCC must have a valid lawful basis, in order to process your personal data.

4.2 Under the UK GDPR there are six lawful bases available, and the one most appropriate to use will depend on our purpose for processing your personal data and our relationship with you.

The six bases are:

- **Consent**
- **Contract**
- **Legal obligation**
- **Vital interests**
- **Public task**
- **Legitimate interests**

5) What personal data do we process

5.1 We process all different kinds of personal data. Personal data, means any data about an individual from which that person can be identified (for example, name or email address) and data which could indirectly identify an individual, meaning that it could identify the individual when combined with other data which we hold about that person (for example, gender or date of birth). It does not include data where the identity has been removed in full (i.e. anonymous data).

***'Personal Data' is defined in Article 4 of the General Data Protection Regulation (GDPR). In practical terms, it means any data handled by the OPCC that relates to an identified or identifiable living individual, directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.**

5.2 The type of personal data we hold will vary depending upon the reason you have had contact with us, but it may include the following:

- Name and address data
- Photograph, Video and Sound and visual images
- Family data
- Lifestyle data
- Social circumstances data
- Education and training data

- Employment data
- Financial data
- Goods or services provided data
- Racial or ethnic origin data
- Political opinions data
- Religious or other beliefs of a similar nature data
- Trade union membership data
- Physical or mental health or condition data
- Sexual life data
- Offences and alleged offences data
- Criminal proceedings data
- Outcomes and sentences data
- Cautions data
- Criminal intelligence data
- Complaint data
- Incident data
- Civil litigation and accident data

5.3 Your personal data may be held on a computer system, in a manual record such as in a physical file, but it can also include other types of electronically held data such as CCTV or body worn video.

6) Special Category Data

6.1 Under UK GDPR, Special Category Data is personal data that is regarded as particularly sensitive and includes the following:

- **Race or Ethnic origin**
- **Political opinions**
- **Religious/philosophical beliefs**
- **Trade union membership**
- **Genetic data - Biological sample**
- **Biometric data - Fingerprint, face recognition, DNA, palm print, iris recognition,**
- **Health**
- **Sex life and Sexual orientation**

6.2 In order to process special category data, we must satisfy not only a valid lawful basis (Article 6 UK GDPR), but also a specific condition for processing sensitive personal data under (Article 9 UK GDPR).

7) What do we use the data for?

7.1 Personal data is held in order to assist the OPCC in carrying out its role in support of the PCC's core statutory functions, some of which are:

- Strategic planning
- Holding the CC to account, including complaint handling
- Partnership working, including local criminal justice partners
- Appointment of OPCC statutory officers
- Appointment, suspension and removal of the CC
- Data and engagement
- Financial processing
- Maintaining our accounts and records
- Promoting our services and activities
- Carrying out research
- Statutory functions, including Freedom of Data Requests and Subject Access Requests (FOI's, SAR''s)
- Processing complaints
- Processing Police Appeal Tribunals and Pension Forfeitures

8) Whose personal data do we handle?

8.1 In order to carry out the purposes described above, the OPCC may obtain, use and disclose personal data relating to a wide variety of individuals including the following:

- Officers and Staff
- Clients
- Suppliers
- Advisers and professional experts
- Complainants, enquirers
- Members of the public
- Individuals captured by CCTV images
- Recipients of Constabulary services
- Elected Officials
- 3rd Party Processors

8.2 The OPCC will only use personal data that is necessary to fulfil a particular purpose or purposes.

9) Method of collecting personal data

9.1 The OPCC collects different types of data from individuals depending upon the reason for their interaction with us and/or the reason why we have collected the data. For ease of reading, we have grouped the main reasons why we collect data into the categories below. Each section explains our reasons and method of collection in more detail.

- Personal data obtained from general correspondence from members of the public and handling casework, and complaints or appeal against the Constabulary, CC, PCC, the Deputy PCC, OPCC staff.
- Processing Anti-Social Behaviour Case Review Appeals (ASBCRA).

- Personal data obtained when processing Police Appeal Tribunals and Pension Forfeitures.
- Personal data obtained during the evaluation and award of PCC grants and/ or commissioned services.
- Personal data obtained as a result of the OPCC's involvement in joint committees and forums.
- Personal data obtained as a result of handling subject access requests under the Data Protection Act 2018, Freedom of Data Act 2000 or the Environmental Information Regulations 2004 (EIR).
- Personal data obtained when individual signs up to receive the OPCC's newsletter or other e-mail newsletters/services.
- Personal data obtained when individuals use our website or other websites we control.
- Personal data obtained when we organise events and take personal photographs or videos at events.
- Personal data obtained when we carry our public consultations.
- Personal data obtained when individuals visit the OPCC.
- Personal data obtained through recruitment of volunteers, OPCC staff and the CC of Derbyshire Constabulary.

10) <u>Who do we share personal data with?</u>

10.1 We may engage the services of commercial companies/processors to store and manage personal data on our behalf. Where we have these arrangements, we will ensure that the requirements of the UK GDPR/DPA2018 on handling personal data are met.

10.2 There are also occasions where we may be required to share your data with other organisations or partners. In order to adhere to our legal obligations and meet our responsibility for the communities we serve. To ensure that our partnership working is effective, we may need to share your personal data with other authorities and partners such as:

- Police and Crime Panel
- Local Authorities
- Home Office
- Derbyshire Constabulary
- Community Groups
- Charities
- Other not for Profit entities
- Contractors
- Employment Agencies
- The Home Office
- Victims Services

10.3 There may also be occasions where we need to share your personal data due to a public safety or security reason such as:

- For the investigation, detection and prevention of a crime.

- Where there is a legal duty to share the data and the importance of doing so outweighs the importance of confidentiality.
- If there are serious risks to an individual, the public, our staff or other professionals
- To protect children or vulnerable adults.
- Any other public interest that outweighs the duty of confidence.

11) Processing activities

11.1 Below is a list of the main areas where processing of personal data is carried out by the OPCC.

General correspondence from members of the public

(Inc. handling complaints against the Constabulary, CC, the PCC, the Deputy PCC and OPCC staff. Complaint Reviews, Anti-Social Behaviour Case Reviews (ASBCR), misconduct proceedings and Police Appeal Tribunals (PAT), Pension Forfeiture.

a) What personal data do we hold?

If you contact us with a general query or complaint against the Constabulary, CC, PCC, Deputy PCC or OPCC staff, or we are processing or facilitating a complaint review, ASBCR, misconduct proceedings, PAT or Pension Forfeiture, you may provide/we may process the following data about you:

- **Identity data** – name, gender, age, marital status, nationality.
- **Contact details data** – address, email address, telephone number.
- **Family data** – data about your family composition and dependants.
- **Third Party data** - data about any third parties' details that are relevant to the purpose of the processing.
- **Special category data** – racial or ethnic origin, mental and physical health, details of injuries or medication/treatment received, political beliefs, religious beliefs, trade union affiliation, genetic data and data concerning sexual life or orientation.
- **Criminal Allegations/Criminal Conviction Data** - data relating to allegations or criminal convictions.

b) How do we collect your personal data?

We will collect data directly from you when you correspond with us by post, telephone, email, on social media or otherwise. Sometimes the data is shared with us as part of a complaint you have submitted to the Constabulary, or as part of misconduct case they are handling, depending on the situation.

c) For what purposes do we use your personal data?

- We will use your data to respond to your query or to investigate your complaint, and to undertake the statutory functions of a PCC. We will also

keep an internal record of your data for audit purposes and lessons learnt reasons.

d) What is the lawful basis for our use of your personal data?

The OPCC is a public authority and has certain powers and obligations regarding responding to members of the public queries and complaints.

The PCC is the voice of the people and therefore, has an obligation under the Police Reform and Social Responsibility Act 2011, to listen to and respond to any queries raised by the public in a timely, thorough manner. Additionally, the PCC has specific statutory duties relating to complaint correspondence and complaint reviews received from members of the public, as described below.

The lawful basis on which we will process your personal data in relating to general correspondence and complaints is under exercise of our official authority and/or in performance of a task in the public interest – under Article 6 (1) (e) UK GDPR.

In relation to processing complaints against the CC our specific obligation can be found in the Police Reform & Social Responsibility Act 2011 and the Police Reform Act 2002.

In relation to processing complaints against the PCC and the DPCC, the specific obligation can be found in the Elected Local Policing Bodies (Complaints and Misconduct) Regulations 2012.

In relation to processing ASBCR's, our specific obligation can be found in the Crime and Policing Bill.

In relation to complaint reviews, our specific obligation can be found in The Policing and Crime Act 2017.

In relation to PAT's, our specific obligation can be found in The Police Appeals Tribunal Rules 2020.

In relation to ASBCR's, our specific obligation can be found in Anti-social Behaviour, Crime and Policing Act 2014.

In relation to the Pension Forfeiture, our specific obligation can be found in The Police Pensions Regulations 1987 and The Local Government Pension Scheme Regulations 2013.

e) On what basis do we use special category data?

The OPCC may sometimes process data about you, which is sensitive, known as Special Category Data (as detailed above). Special Category Data requires higher levels of protection, and we must have a further justification for processing this type of personal data than we do for standard personal data.

We will only process this type of data on the basis that one of the following applies:

- **Received explicit consent from the data subject**
- **In relation to employment, social security and social protection (if authorised by law)**
- **To protect vital interests**
- **Relating to not-for-profit bodies**
- **Data has been made manifestly public by the data subject**
- **To defend or bring legal claims or judicial acts**
- **It is necessary for reasons of substantial public interest (with a basis in law)**
- **Relating to health or social care (with a basis in law)**
- **Relating to public health (with a basis in law)**
- **For archiving, research and statistical purposes (with a basis in law)**
- **To satisfy the statutory duties of the PCC**

In some circumstances we may need to approach you for written consent, to allow the OPCC to process certain types of sensitive personal data. In these circumstances, you will be provided with full details of the personal data that is required and why it is needed, to allow you to carefully consider whether you wish to consent.

What is meant by 'consent'

The UK GDPR sets a high standard for consent – this means that organisations such as the OPCC must offer individuals real choice and control over their personal data where consent is the lawful basis for processing.

Much of the data processed by the OPCC uses consent as the lawful basis, and the OPCC recognises that managing this is essential for accountable compliance with data protection legislations and law, and for building trust and confidence with the public.

To be valid, consent must be:

- **Freely given** – The data subject must have a genuine choice without pressure or coercion. It cannot be a pre-ticked box or a condition for receiving a service that the person needs.
- **Specific –** Consent must be for specific, clearly defined purposes. If you have multiple reasons for processing data, you must get separate consent for each processing activity.
- **Informed –** The data subject must be fully aware of your identity, the purposes of the data processing, and what will be done with their data. This data must be provided in clear, plain language.
- **Evidenced** – a record should be kept re: who, when how and what individuals were told about the processing.
- **Unambiguous** – Consent requires a clear affirmative action, such as ticking an opt-in box, signing a form, or clicking a button. It cannot be assumed from silence or pre-checked boxes.
- **Easy to withdraw** – It must be as easy for the data subject to withdraw their consent as it was to give it. This must be explained to them upfront, and mechanisms for withdrawal must be provided to the data subject.

(If you have given consent for the OPCC to process your personal data and you have changed your mind – please contact the OPCC via the details at the bottom of this notice to advise that you wish to withdraw your consent. The OPCC will then liaise with you to discuss further).

f) Who will we share your personal data with?

We may share your personal data with third parties if it is necessary to resolve your query, complaint or appeal etc; or they are dealing with your query, complaint or review on your behalf.

We may share your personal data with the Constabulary where we are required to gather further data or are legally required to do so, or we have a safeguarding concern.

We may share your personal data with the Independent Office of Police Conduct (IOPC), if a complaint requires a mandatory referral to them, or to seek appropriate advice from them.

We may share your personal data with the Police and Crime Panel if a complaint is recorded against the PCC or a DPCC, as they are the relevant authority who would investigate those complaints, not the OPCC.

We will share your data with the services providers of our OPCC correspondence recording systems Contensis developed by Zengenti. More data can be found on their website - Zengenti – creators of the Contensis content management system.

We may share your personal data with the relevant council/s to process your ASBCR application - ASB Case Review MOU.

We my share your personal data with external legal bodies (barristers/solicitors/the Courts) relating to PAT's where we are legally required to do so.

We may share your personal data with The Home Office and the relevant Pension Administrator, if we are processing a pension forfeiture.

We may share your personal data with Sancus, if we are utilising their services in relation to complaint reviews. More data can be found on their website - Investigative Training & Review Services | Sancus Solutions

j) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Grants and commissioned services

a) What personal data do we hold?

If you (or your organisation) apply for a grant or to enter into a contract with the OPCC, we may collect some personal data about the individuals who work or volunteer at the applicable organisation. Although most details relating to organisations do not constitute personal data, if your organisation is a partnership or you are a sole trader, it is likely that most of the data that you provide to us will be personal data. The data we typically collect from applicants is:

- **Identity data–** name, job title
- **Contact details data** – address, email address, telephone number
- **Liability data -** regarding contract/pension
- **DBS data**
- **Financial data** – bank account details

b) How do we collect your personal data?

We collect the above data via submission of electronic documents sent to us from you via email or post.

c) For what purposes do we use your personal data?

- We only use your data for the purpose of evaluating and awarding PCC grants and/or commissioned services. We will keep a record of this data internally for monitoring purposes, and some of the contract data and your organisation's name will be published on the OPCCs website if you are successful in securing a grant/contract; this is published to aid with our transparency requirements.

What is the lawful basis for our use of your personal data?

The OPCC is a public authority and has certain powers and obligations under the Police Reform & Social Responsibility Act 2011, which allows the OPCC to award crime and disorder reduction grants. Therefore, the lawful basis on which we will process your personal data is in the exercise of our official authority and/or in performance of a task in the public interest - under Article 6 (1) (e) UK GDPR.

In respect of awarding contracts and commissioning services, our lawful basis for processing your personal data will be on the basis that it is necessary for the performance of a contract or to take steps to enter into a contract - under Article 6 (1) (b) UK GDPR.

d) Who will we share your personal data with?

We will not share your personal data with any third party (except that your organisation's name/your name will appear on our website for transparency purposes if you are successful).

e) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Business Crime Reduction Partnership (BCRP)

a) What personal data do we hold?

If you (or your organisation) enter into a contract with the BCRP to become a BCRP Member, we may collect some personal data about some of your employees, this will normally be those individuals who will be using the DISC system to report business related crimes into the BCRP.

The data we typically collect from the businesses is:

- **Identity data–** name, job title etc.
- **Contact details data** – work address, work email address, contact telephone number
- **Financial data** – bank account details of the business (if applicable)

Additionally, the BCRP will process personal data relating to offenders. This data will be processed through the DISC system.

This data is –

- General statistical data relating to the number and types of offences occurring within the geographical area in which the BCRP operates.
- Details of offenders convicted of relevant retail-related offences, including shop theft, fraud, business robbery, business burglary, and violence committed within a retail setting.
- Custody images of offenders convicted of relevant offences where sharing is necessary and proportionate for crime prevention purposes.
- Details and photographs of individuals who are subject to court orders restricting their access to, attendance at, or presence within retail premises or retail areas.
- Information relating to individuals identified as High Harm Offenders in accordance with the Tackling Retail Crime Together Strategy. A High Harm Offender is an individual who has been charged with at least one relevant offence within the previous six months and continues to commit or is suspected of continuing to commit relevant offences.

- Offender information from the BCRP members (i.e. CCTV footage etc.). Offender's name, date of birth, distinguishing marks/traits and facial image and any relevant data about the nature of his/her activities, associates; the purpose of this processing is to enable members to identify offenders in order to submit reports about them, and to provide data about them which may be necessary to protect the property and personal safety of members and their staff, customers etc.
- Criminal activity data - the purpose of this processing is to enable the Scheme to collate intelligence on criminal activity within the area of the Scheme's operation and to inform the members of the Scheme, so that they can take the necessary precautions to 15 protect staff and stock from harm and criminality. Such data may be shared with Members.

b) How do we collect your personal data?

We collect the above data via submission of electronic documents sent to us from you via email or post when signing up to be a BCRP Member, or via the DISC system if related to offenders or subjects of interest.

c) For what purposes do we use your personal data?

We only use the data for the following purposes –

- Running an effective business crime reduction partnership, for example - administering DISC access etc., and processing offender/persons of interest data.

What is the lawful basis for our use of your personal data?

Article 6 UK GDPR - Lawful Basis

- **Recognised Legitimate Interest** (Data Use and Access Act 2025 – Crime Prevention - prevention, detection or investigating crimes, as long as not to perform your tasks or functions).

Article 9 UK GDPR – Condition for Processing

- **Special Category Data - Reasons of substantial public interest** (requires a basis in law). Crime Prevention - prevention, detection or investigating crimes.

Article 10 UK GDPR/Schedule 1 of DPA 2018 – Condition for Processing

- **Criminal Offence Data - Reasons of substantial public interest** - Preventing or detecting unlawful acts. Crime Prevention - prevention, detection or investigating crimes.

d) Who will we share your personal data with?

The BCRP team utilise the DISC system for reporting, therefore offender/persons of interest data will be processed using this system and shared with BCRP Members/partners and the Constabulary via this system.

Additionally, data relating to BCRP membership, will be processed using the DISC system, and the OPCCs internal systems.

e) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Holding to account

a) What personal data do we hold?

We attend various meetings and data sharing forums with other public sector bodies as part of our public duties to secure an efficient and effective police force, bring together community safety and criminal justice partners, and to make sure local priorities are aligned. This includes the Commissioner's Public Assurance Meetings (PAM).

Personal data is obtained from the Constabulary and other third parties as a result of the OPCC's involvement in joint committees, meetings and forums.

Examples of the types of committees, meetings and forums that we attend are:

- Briefings from the Constabulary, or the CC directly.
- Police station visits attended by the PCC and OPCC staff.
- Meetings with the CC attended by the PCC, officers and OPCC staff (for example the Commissioner's PAM).
- Partnership meetings with the PCC.

During the course of these meetings, we may obtain personal data about members of the public, victims, offenders and their family members. In addition, to facilitate the Public Questions element of the Commissioner's Public Assurance Meeting it is necessary for us to obtain personal data about yourself, so we can contact you to clarify or respond to any questions or queries raised. The data you may provide/we may process will be:

- **Identity data** – name, gender, age, marital status, nationality.
- **Contact details data** – address, email, telephone number.
- **Family data** – data about family composition and dependants.

- **Special category data** – racial or ethnic origin, mental and physical health, details of injuries or medication/treatment received, political beliefs, religious beliefs, trade union affiliation, genetic data and data concerning sexual life or orientation.
- **Criminal offence data** - details of criminal convictions, arrests, and cautions

b) How do we collect your personal data?

For personal data obtained through committees, meetings and forums, data will generally be verbally given, but can be collected in minutes of meetings, briefing notes, telephone calls, data sent electronically to us or obtained in hard copy at such meetings.

For Public Assurance Meetings, personal data is collected via MS Forms, this enables respondents to submit their questions to the Chief Constable or the PCC, and to provide us with their contact details for a response. Respondents are asked whether they consent to the OPCC sharing their name and contact details with Derbyshire Constabulary, in the event that the Constabulary need to contact the requester directly for operational policing purposes.

c) For what purposes do we use your personal data?

The purpose of our attendance at such meetings (and subsequent collection of personal data) is generally to hold the CC to account, which is part of the PCC's statutory duties.

For Public Assurance Meetings, we may use your personal data to clarify, and in some cases respond to, questions submitted.

d) What is the lawful basis for our use of your personal data?

The PCC has an obligation under the Police Reform & Social Responsibility Act 2011 to hold the CC to account, which involves the OPCC attending meetings to understand the progress made towards the Police and Crime Plan, and the general running of Derbyshire Constabulary as a whole. Therefore, the lawful basis on which we will process your personal data is in the exercise of our official authority and/or in performance of a task in the public interest - under Article 6 (1) (e) UK GDPR.

e) On what basis do we use special category data?

The OPCC may sometimes process data about you, which is sensitive, known as special category data (as detailed on page 7 of this Privacy Notice).

Special category data requires higher levels of protection, and we have to have further justification for collecting, storing and using this type of personal data.

We will only process this type of data during the course of our involvement in joint committees, forums and meetings on the basis that:

- **We have received explicit consent from the data subject**

- **In relation to employment, social security and social protection (if authorised by law)**
- **To protect vital interests of an individual**
- **Relating to not-for-profit bodies**
- **Data has been made manifestly public by the data subject**
- **To defend or bring legal claims or judicial acts**
- **It is necessary for reasons of substantial public interest (with a basis in law)**
- **Relating to health or social care (with a basis in law)**
- **Relating to public health (with a basis in law)**
- **Relating to legal claims**
- **For archiving, research and statistical purposes (with a basis in law)**

In some circumstances we may need to approach you for written consent, to allow the OPCC to process certain types of sensitive personal data. In these circumstances, you will be provided with full details of the personal data that is required and why it is needed, to allow you to carefully consider whether you wish to consent.

f) On what basis do we use data about criminal convictions?

Data about criminal convictions requires higher levels of protection and we need to have a further justification for collecting, storing and using this type of personal data.

We will only process this type of data during the course of our involvement in joint committees, meetings and forums on the basis that:

- It is necessary for reasons of substantial public interest; or
- It is necessary for the establishment, exercise or defence of legal claims; or
- The data has been made public by the individual; or
- It is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- It is necessary for safeguarding reasons.

g) Who will we share your personal data with?

Residents submitting questions to the Public Assurance Meetings are asked whether they consent to the OPCC sharing your name and contact details with Derbyshire Constabulary in the event they wish to investigate any issues raised further.

Please note that as we will usually obtain the above data via our attendance at multi-party meetings, these organisations are likely to hold the applicable personal data also, and they may separately share your personal data with third parties.

h) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Subject Access and Freedom of Data requests

a) What personal data do we hold?

If you contact us with a request for data (such as a Subject Access Request (SAR), Freedom of Information request (FOI), or Environmental Information Request (EIR), then the data you may provide/we may process will be:

- **Identity data** – name, gender.
- **Contact details data** – address, email address, telephone number.
- **2 forms of ID** - for SAR.

You may also provide the OPCC other data relating to you, so that we can identify the data you have requested.

b) How do we collect your personal data?

We will collect data directly from you when you request the information. You will correspond with us by post, telephone, email, phone, social media or otherwise.

c) For what purposes do we use your personal data?

- We use your data to respond to your data request. We will keep an internal record of your data for audit reasons.

d) What is the lawful basis for our use of your personal data?

We will process your personal data relating to your request for data on the basis that we have a legal obligation – under Article 6 (1) (c) UK GDPR, to provide that data or respond to your data request as a public authority.

In relation to processing SAR's, our specific obligation can be found in the UK General Data Protection Regulations and the Data Protection Act 2018.

In relation to processing FOI's, our specific obligation can be found in the Freedom of Data Act 2000.

In relation to EIR's, our specific obligation can be found in the - The Environmental Data Regulations 2004

e) Who will we share your personal data with?

We will only share your personal data with third parties if it is necessary to respond to your data request, such as where they hold relevant data that we are required to provide to you, or in order for us to provide a response to your enquiry. We may need to liaise with the Constabulary or other agencies in order to establish facts or supporting data. We may also need to liaise with the Data Commissioner's Office (ICO) in certain circumstances.

f) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Please note - In many cases, it will be the Chief Constable (CC) of Derbyshire Constabulary and not the PCC who holds personal data on the Police National Computer (PNC) relating to prosecutions, convictions and cautions. The CC is therefore the Data Controller of this data, not the PCC. Any data requests relating to operational policing or PNC requests should therefore be sent directly to the Constabulary, not the OPCC for a response, using their online FOI/SAR form, or by calling 101.

OPCC managed websites and Social Media Channels

a) What personal data do we hold?

The OPCC manages three websites, the main PCC website, Derbyshire Victim Services and the DPARC Rural Crime Prevention Hub

When you visit a website or social media channel managed by the OPCC, we may automatically collect technical data about your equipment, browsing actions and patterns from your computer (for example, internet protocol (IP) addresses, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other data on the devices you use to access our website.

If we do collect other personal data through our websites, we will be upfront about this. We will make it clear when we collect personal data, and we will explain what we intend to do with that personal data.

b) How do we collect your data?

There are two main ways in which we collect your personal data: -

i. Analytics

When you visit www.Derbyshire-pcc.gov.uk, www.derbyshirevictimservices.co.uk or, www.derbyshireruralcrimehub.org.uk, we use a third-party service, Google Analytics, to collect standard internet log data and details of visitor behaviour patterns. We do this to find out such things as the number of visitors to the various parts of the site which gives us insight into which parts of our website is being utilised the most by the public. This data is only processed in a way that does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website.

ii. Cookies

Cookies are small text files stored on your device to make browsing easier by remembering preferences and improving site performance. The OPCC uses cookies for Google Analytics (GA4) to enhance user experience and for the Font Size selector on the accessibility page to retain your chosen settings.

You can read more about how we use cookies on our Cookies policy at the bottom of the OPCC's website - Policies, Procedures and Guidance Documents | Office of the Derbyshire Police and Crime Commissioner

c) For what purposes do we use your personal data?

The purpose for implementing all of the above is to maintain and monitor the performance of our websites, uphold network security and to constantly look to improve the site and the services we offer to our users.

d) What is the lawful basis for our use of your personal data?

The lawful basis we rely on to process your personal data is legitimate interests - under article 6(1)(f) of the UK GDPR. In this case, the legitimate interest would be for us to process your personal data for the running of our website, provision of administering IT services and network security.

e) Who will we share your personal data with?

We will only share your data with third party provider Zengenti ltd, who provide the Contact Management System solution for the Office of the PCC of Derbyshire. We will utilise their casework system should we need to respond to any social media enquiries.

Please note that where we provide links to websites of other organisations, plug-ins, and applications. Clicking on those links or enabling these connections may allow third parties to collect or share data about you. We do not control these third-party websites, and this privacy notice does not cover how these websites, organisations or applications processes personal data. We encourage you to read the privacy notices on the other websites you visit.

The internet is not a secure medium, and the OPCC cannot absolutely guarantee the security of your personal data provided over the internet. However, we have put in place various security measures to help mitigate the risk of your personal data. Our website and associated databases are protected by certified firewalls to protect your personal data from access by unauthorised persons and against unlawful processing. We also keep your personal data confidential. All outgoing and incoming emails are scanned for viruses.

f) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Media enquiries

a) What personal data do we hold?

We receive enquiries from the media on current affairs, the work of the PCC as well as policing, criminal justice and community safety matters. In addition, we publicise the work of the PCC through the issuing of press releases and other publications.

In order to reply to media enquiries, we need enough data from the representative of the media, in order to provide a response. This will include their name, telephone number/contact email address and, where relevant, the name of the organisation they represent, as well as the details of the enquiry.

We maintain a list of email addresses for media and community contacts who have requested our press releases.

b) How do we collect your data?

We will collate this data when contacted by a representative of the media, usually by telephone or email or sometimes in person. We will only take enough data to provide a response or to add them to our press release distribution list, if requested.

c) For what purposes do we use your personal data?

We need to keep a record of who we have spoken with and what has been asked for/provided. If we cannot answer your query/request over the phone, we will need your contact data to enable us to get a response to you via another route.

We will only use your personal data to respond to you and will make a record of our communications with you, both verbal and written.

We will also use your contact data to send you our press releases, if requested.

d) What is the lawful basis for our use of your personal data?

The OPCC have an obligation under the Police Reform & Social Responsibility Act 2011 to hold the CC to account, and part of this is communicating to the public via social media and media enquiries what activities and actions have been taken by the CC and the PCC to address issues raised. Therefore, the lawful basis on which we will process your personal data is in the exercise of our official authority and/or in performance of a task in the public interest - under Article 6 (1) (e) UK GDPR.

e) Who will we share your personal data with?

In order to provide a response to your enquiry, we may need to liaise with the Constabulary or other agencies/partners in order to establish facts or supporting information.

Some data may be shared with the PCC's external communications provider Better Times - Better Times Limited - Better Times Limited. This is so they can provide advice and support to the PCC as needed.

f) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

You can, however, ask us to stop sending you press releases at any time, and we will stop immediately, and update our records to reflect your wishes. You can do this by contacting the OPCC (details at the end of this notice).

Public consultations, Focus Groups and Event Booking Forms

a) What personal data do we hold?

The exact nature of the personal data collected when you respond to our consultations or attend our focus groups or events will vary, but in general will be relevant personal contact details and, for consultations, your opinions relating to the subject area being discussed. In all cases, personal data will be limited only to data which is necessary to understand the specific subject area being consulted upon and for demographic monitoring purposes.

We may publish a summary of the consultation responses and/or some analytical data, but this will not contain any personal data.

b) How do we collect your personal data?

Most of our consultations, focus groups and event booking forms are conducted online through web-based surveys and online meetings, though alternative paper-based versions of survey questions may also be provided for those who require them.

Some consultations, focus groups and events may also be conducted face-to-face. Where this is the case, we will be clear on what personal data will be collected and how it will be handled.

c) For what purposes do we use your personal data?

The OPCC conducts public consultations in order to inform its work and services. The PCC also has statutory obligations to consult with the public to gather their views. The Police Reform and Social Responsibility Act 2011, together with other legislation, places a legal obligation on the OPCC to: -

- Obtain the views of local people on policing and have regard to those views.
- Make arrangements for engaging with local people in setting police and crime objectives.
- Obtain the views of local people and ratepayers prior to setting the police precept and the policing budget.
- Obtain the views of victims of crime about matters concerning local policing and, where appropriate, feedback to them on actions taken to address them.

We collect demographic data (such as home postcode, gender, age range and ethnic grouping) to assist with obtaining a representative sample of responses, and to ensure that responses are from residents of the Derbyshire Constabulary area. Provision of this data will always be optional and is not required in order to complete a consultation.

In addition, the OPCC collects personal data for the purposes of organising and conducting focus groups and PCC-led events. This data is collected in order facilitate event logistics, such as confirming attendance, providing accessibility arrangements, and sharing relevant materials and follow-up communications relevant to the topic under discussion.

d) What is the lawful basis for our use of your personal data?

The OPCC have an obligation under the Police Reform & Social Responsibility Act 2011 to ensure that the PCC consults with the public on a regular basis, especially around the Precept and the Police and Crime Plan priorities. Therefore, the lawful basis on which we will process your personal data is in the exercise of our official authority and/or in performance of a task in the public interest - under Article 6 (1) (e) UK GDPR.

e) Who will we share your personal data with?

Data may be collected via Microsoft Forms, Brevo, Mentimeter or Eventbrite – Eventbrite. Results from the surveys are published in the public domain but do not contain any personal data. If survey data is shared with partners, then it is anonymised before it is shared.

f) How long will we keep your personal data?

Summaries of the responses to consultations may be published and remain available indefinitely, or as per statutory requirements, but these will not include any personal data.

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Photographs and filming

a) What personal data do we hold?

Photographs and/or video recordings of you (together referred to as "images") will constitute personal data if you can be identified from the photograph and/or recording.

When we take images of you, we will ask you to complete a form to record your consent for us to use them for marketing and publicity purposes or, optionally, for another other stated reason. If you consent for us to do so, we will hold your images, along with the data provided on the consent form.

For children under 16 years of age, we will additionally seek parental consent for images to be used.

b) How do we collect your personal data?

Your personal data may be collected in images taken at events you attend and through the consent form that we will ask you to complete.

c) For what purposes do we use your personal data?

We will only use your images for the specific purposes detailed in the consent form for which you have consented to.

d) What is the lawful basis for our use of your personal data?

The lawful basis that we rely on to process your personal data is consent – under Article 6 (1) (a) UK GDPR, as you would be consenting to your image being used by the OPCC.

You have the right to withdraw your consent for processing at any time. You can do this by contacting the OPCC directly (details at the end of this privacy notice).

Once we have received notification that you have withdrawn your consent, we will delete any images of you and not include such images in any future publications or other materials. However, we will not be able to remove your images from publications that have already been circulated. As at that time, you consented to us processing your images.

e) Who will we share your personal data with?

The OPCC will share your images with third parties, specifically those listed on the consent form (i.e. media contacts when issued with a press release, the Commissioner's monthly newsletter and social media channels, printing organisations). Third parties may however receive your images by virtue of them receiving or accessing the applicable publication in print or online.

Images may also be edited or processed using third-party design or media-editing software, such as Canva, Orla, Adobe products, or similar tools, for the purpose of producing communications materials for the OPCC. Some of these organisations are outside the UK/EU; therefore, personal data may be processed outside of the UK.

f) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Visiting the office

a) What personal data do we hold?

We meet visitors at our office, including:

- dignitaries
- members of the public (by prior appointment)
- journalists.
- external training providers
- job applicants
- suppliers and tradespeople
- stakeholders and key partners
- volunteers and groups

We may retain the name of visitors and details of the organisations they represent for an audit trail. On diary entries we may additionally record details of topics to be discussed at the meeting and/or any necessary supporting information.

b) How do we collect your data?

We ask all visitors to sign in and out at the OPCCs Head Quarters reception. We may also keep a record of preplanned appointments in the electronic diary of the relevant staff member(s) being visited.

c) For what purposes do we use your personal data?

We gather this data for security, fire safety and audit purposes and to enable efficient functioning of the office.

d) What is the lawful basis for our use of your personal data?

The lawful basis we rely on to process your personal data is legitimate interests – under Article 6(1)(f) of the GDPR, which allows us to process personal data when it is necessary for the purposes of our legitimate interests. In this case, our legitimate interest would be to record who is visiting the Constabulary's Head Office site for security and safety reasons, and to record any meetings undertaken with the Commissioner or OPCC staff with third parties for audit purposes.

e) Who will we share your personal data with?

We may share some of this data with the Constabulary if necessary to the meeting/reason for visiting.

f) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

Applying for a job, committee or volunteer role

a) What personal data do we hold?

If you apply for a job, or committee/volunteering opportunity with us, we will ask you to complete an application form, which includes a separate equal opportunity monitoring form.

We may collect the following data on the application and equal opportunities forms:

- **Identity data** – name.
- **Contact details data** – address, email address, telephone number.
- **Medical data** – sickness absence, disabilities or reasonable adjustments required.
- **Equal opportunities data** - racial or ethnic origin, mental and physical health, political beliefs, religious beliefs, trade union affiliation, genetic data and data concerning sexual life or orientation. Please note that you do not have to provide this data and it will not affect your application. We will not make the data available to any staff outside our recruitment team, including hiring managers, in a way that can identify you. Any data you provide will be used to produce and monitor equal opportunities statistics.
- **Criminal offence data** - details of criminal convictions, arrests and cautions.
- **Financial details** – paying expenses etc.

If you are applying for an OPCC staff role or the CC role, if successful, you will be asked to complete a medical questionnaire. This will include:

- **Medical data** - medical history, details of medication/treatment received, sickness absence, disabilities.
- **Vetting data** – criminal convictions data, financial data, family member data etc**.**

The above human resources processes are normally carried out by the Constabulary, not the OPCC. The Constabulary's vetting form has a separate privacy notice setting out how your personal data will be processed in regard to the vetting processes.

b) How do we collect your personal data?

We will collect the above personal data from the information you provide on your application form, and any other correspondence in relation to your application.

c) For what purposes do we use your personal data?

- Our purpose for processing this data is to assess your suitability for a role you have applied for with the OPCC.

- The data is processed under a contractual obligation in order for the OPCC to run a fair and efficient recruitment process, and prior to the data subject entering into an employment contract with the OPCC.

- It is also utilised to ensure that the OPCC recruit only individuals that satisfy the required standards relating to security and vetting clearance.

d) What is the lawful basis for our use of your personal data?

If you are applying for a job with the OPCC (excluding the CC role), the lawful basis we rely on for processing your personal data is that it is necessary to performance of a contract – under Article 6 (1) (b) UK GDPR, or to take steps at your request before entering into a contract of employment with the OPCC.

If you are applying for a volunteering opportunity with the OPCC, the lawful basis we rely on for processing your personal data is legitimate interests – under Article 6(1)(f) of the GDPR. In this case, the legitimate interest would be to ensure that you are fit for the role you will be undertaking and that the relevant checks can be undertaken prior to you starting the volunteering.

If you are applying for the role of CC, the lawful basis on which we process your personal data is in the exercise of our official authority and/or in performance of a task in the public interest – under Article 6 (1) (e) UK GDPR. The PCC's specific duty regarding recruitment of a CC can be found within the Police Reform and Social Responsibility Act 2011.

e) On what basis do we use special category data?

The OPCC may sometimes process data about you, which is sensitive, known as special category data (as detailed above).

Special category data requires higher levels of protection, and we need further justification for collecting, storing and using this type of personal data.

The lawful basis we rely on to process any data you provide as part of your application which is special category data, such as health, religious or ethnic data is under Article 9(2)(b) of the UK GDPR, which also relates to our obligations in employment and the safeguarding of your fundamental rights, and Article 9(2)(h) UK GDPR for assessing your work capacity as an employee. Schedule 1 part 1(1) and (2)(a) and (b) of the DPA 2018 also which relates to processing for employment, the assessment of your working capacity and preventative or occupational medicine.

f) On what basis do we use data about criminal convictions?

Data about criminal conviction requires higher levels of protection and we need to have a further justification for collecting, storing and using this type of personal data.

We will only process this type of data during the course of evaluating your application on the basis that should an offer of employment be made, successful police vetting will be required for the individual to gain access to Constabulary data, equipment, and assets.

The lawful basis we rely on to process any data about your criminal convictions when you apply for a job is Schedule 1 part 1 (1) of the DPA 2018 which relates to processing for employment purposes and the assessment of your working capacity.

g) Who will we share your personal data with?

We will share your personal data with the following parties:

- Derbyshire Constabulary HR team (as the OPCC uses the services of their HR team for OPCC HR applications).
- Derbyshire Constabulary Vetting Unit (for processing the police vetting form).
- Any other relevant partners for the purposes of security and vetting clearance, like the UK government/INTERPOL.

In relation to the appointment of the CC and senior OPCC post holders, we may also share your personal data with the following parties:

- Home Secretary (CC only).
- Police and Crime Panel (as they have a statutory role in relation to the review of OPCC senior appointments).
- College of Policing (if we use their services to aid the recruitment process).
- Independent interview panel members (as notified to you in advance).

h) How long will we keep your personal data?

For more data about how long we hold personal data see our retention schedule on the policies page on our website, or please contact the OPCC via the details at the end of this notice.

12) Failure to provide personal data

If you fail to provide certain data when requested, we may be prevented from complying with our statutory functions (such as complaint handling, FOI/SAR, grants etc) and we may be unable to respond adequately or provide the right assistance to you.

13) Sharing your personal data

The identity of any third parties with whom we may share your personal data is set out in each specific circumstance of data collection detailed above. The OPCC may also share your data with some, or all of the following (but only where necessary):

- Other public sector bodies the OPCC works with, for example, Derbyshire Constabulary, Derbyshire County Council, MP's.
- OPCC agents, suppliers and contractors.
- On occasion, local authorities or not for profit bodies with which the OPCC is carrying out joint ventures, e.g. in relation to facilities or events for the community.

These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly regarding the manner in which they process and protect your personal data.

14) How long is personal data retained?

For more data about how long we hold personal data and see our retention schedule on our policies page on our website, or please contact the OPCC via the details at the end of this notice.

Please note that we have certain statutory obligations to retain some personal data in connection with our statutory obligations as a public authority.

We may also retain data in order to defend or pursue legal claims. In some cases, the law imposes a time limit for such claims, therefore the OPCC will retain some personal data for this purpose, if it is believed to be necessary to be able to defend or pursue a legal claim.

In general, the OPCC will endeavour to keep personal data only for as long as it is required. This means that the data will be deleted as soon as it is no longer needed.

15) Your Individual Rights

There are a number of Individual Rights in relation to your personal data, which data subjects are entitled to exercise, as outlined below.

When you seek to exercise any of your individual rights, the OPCC will require a data form to be completed, and identification will be required. The form can be found on our website

- https://www.derbyshire-pcc.gov.uk/Transparency/FreedomofData/Information-Request-Form.aspx

Alternatively, you can email the OPCC on – PCCOffice@Derbyshire.PNN.Police.UK or call the OPCC on – 0300 122 6000

You have the following rights with respect to your personal data:

Right to be Informed

You have the right to be informed about the collection and use of your personal data.

We will endeavour to provide data, which is concise, transparent and easy to understand. We must provide you with data including:

- Our purposes for processing your personal data.
- How long we keep your personal data (i.e., the retention periods).
- Who it will be shared with.

We call this ‘privacy data’ and this data is contained within this privacy notice.

We must provide privacy data to you at the time we collect your personal data. The OPCC’s email address has an automatic acknowledgement that contains the link to our privacy notice.

If we obtain personal data from other sources, e.g., third parties, then we must provide you with privacy data within a reasonable period of obtaining the data, and no later than one month after the data was obtained. However, there are a few circumstances in which we do not need to provide you with privacy data, these are if you already have the data or if it would involve a disproportionate effort to provide it to you.

All privacy data provided to you by the OPCC should be concise, transparent, intelligible, easily accessible, and it must be in clear and plain language.

We regularly review, and where necessary, update our privacy data. If we have any new uses of your personal data, we will bring this to your attention before we start processing that data.

Please also note, that there may be occasions when it is necessary and proportionate to restrict the provision of data in the context of law enforcement. Therefore, we might not supply you with privacy data if this would undermine or be in breach of the law.

Right of Access

This is commonly known as subject access. You can submit a Subject Access Request (SAR) to:

- Confirm whether your data is being processed
- Gain access to your personal data
- Verify the lawfulness of the processing; and
- Access other supplementary data – however all other data should be detailed in this notice.

Subject Access Requests can be made verbally or in writing and will be free of charge, unless we consider your request to be:

- Manifestly unfounded, or
- Excessive or repetitive.

If we deem one of the above to be the case, we may request a reasonable fee or refuse to process your request. If a fee is applied this will be based on the administrative cost of providing the data to you.

We must provide you with your data within one month of receiving your subject access request. However, we can lawfully extend this by a further two months if your request is complex or you have submitted numerous requests to us. If there is a delay in dealing with your request, we will inform you within one month of receiving your request and we will explain why the extension is necessary.

We may also be required to ask you for documents to prove your identity. If this is required, then the one month will commence from the date your proof of identity is confirmed to us.

If we refuse to process your request, we will explain why and inform you of your right to an internal review of that decision. Thereafter, your right to complain to the Data Commissioner's Office (ICO) within one month of receipt.

More details regarding information requests can be found in our Access to Information Policy - Policies, Procedures and Guidance Documents | Office of the Derbyshire Police and Crime Commissioner

Right to Rectification

You are entitled to have personal data rectified if it is inaccurate or incomplete.

Requests for rectification will be responded to within one month of receipt, however if we believe your request to be manifestly unfounded or excessive then we may request a reasonable fee in order to process your request, or we may refuse to deal with your request altogether. The fee will be based on the administrative costs of complying with your request

If we decide to charge a fee, we will also notify you within one month of receipt, however we will not comply with you request until the fee is received.

We may also be required to ask you for documents to prove your identity. If this is required, then the one month will commence from the date your proof of identity is confirmed to us.

We do have the right to extend the time to respond to your request by a further two months if your request is complex or you have submitted numerous requests. We will write to you to advise you of the delay within one month of receiving your request.

If we decide not to act in response to your request for rectification, we will explain why and inform you of your right to an internal review, and thereafter, to complain to (ICO). We will do this within one month of receiving your request.

If we have disclosed personal data deemed as inaccurate or incomplete to others, then we will contact the recipient(s) and inform them of the rectification, unless to do so proves impossible or involves disproportionate effort.

Right to Erasure/to be Forgotten

The right to erasure is also known as *'the right to be forgotten'*. This right enables you to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure is not an absolute right and only applies in the following circumstances.

- Your personal data is no longer necessary for the purpose which we originally collected or processed it for.
- We relied on your consent as your lawful basis for holding the data, and you now wish to withdraw your consent.
- We relied on legitimate interests as our reason for processing your personal data and you now object to us processing your data, and we have no overriding legitimate interest to continue this processing.
- We are processing your personal data for direct marketing purposes and you object to that processing.
- We have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the first principle).
- We have to do it to comply with a legal obligation.

We will respond to your request for your right to erasure within one month, however this can be extended by two months where the request is complex, or if we receive a number of requests from you. We will inform you within one month of the receipt of the request and explain why the extension is necessary

We may also request a reasonable fee or refuse to comply with your request for erasure if we consider it is manifestly unfounded or excessive. We will write to you within one month of receipt of your request and explain our decision. Any fee will be based on the administrative costs of complying with the request. If we charge a fee, then your request will not be processed until the fee is received.

If we refuse to process your request, we will explain why and inform you of your right to an internal review, and thereafter, to complain to the (ICO), within one month of receipt.

There are some specific circumstances where the right to erasure does not apply, and therefore a request may be refused. These reasons could involve data processed for the following purposes:

- To exercise the right of freedom of expression and data.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research historical research or statistical purposes.
- The exercise or defence of legal claims.

If we have disclosed your personal data to others, and then subsequently determine that your right to erasure is valid, we will contact the recipient(s) of your data and inform them of the erasure, unless to do so proves impossible or involves disproportionate effort.

Right to Restrict

Individuals have a right to *'block'* or suppress processing of personal data.

When processing is restricted, organisations are permitted to store the personal data, but not further process it.

Organisations can retain just enough data about the individual to ensure that the restriction is respected in future.

The right to restrict processing is not an absolute right and only applies in certain circumstances.

We are required to restrict the processing of your personal data in the following circumstances:

- Where you contest the accuracy of your personal data, we must restrict the processing until we have verified the accuracy of your personal data.
- We have unlawfully processed your personal data, and you oppose the erasure and request restriction instead.
- We no longer need the personal data, but you need us to keep it in order to establish, exercise or defend a legal claim.
- You have objected to us processing your personal data under Article 21(1), and we are considering whether our legitimate grounds override your right to object.

We will respond to your request for restriction within one month, however this can be extended by two months where the request is complex, or we receive a number of requests. We will inform you within one month of the receipt of the request and explain why the extension is necessary

We may also request a reasonable fee or refuse to comply with your request for restriction if we consider it is manifestly unfounded or excessive. We will write to you within one month of receipt of your request and explain our decision. Any fee will be based on the administrative costs of complying with the request. If we charge a fee, then your request will not be processed until the fee is received.

If we refuse to process your request, we will explain why and inform you of your right to an internal review, and thereafter, to complain to the Data Commissioner's Office (ICO), within one month of receipt.

If we have disclosed personal data to others, and then subsequently determine that your right to restriction is valid, then we will contact the recipient(s) and inform them of the restriction, unless to do so proves impossible or involves disproportionate effort.

We will also advise you when the restriction on processing is lifted.

Right to Data Portability

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services.

It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- To personal data you have provided to a data controller,
- Where the processing is based on your consent or for the performance of a contract, and
- When processing is carried out by automated means.

We will provide your personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the data is structured so that software can extract specific elements of the data. If requested and technically feasible we will transmit the data directly to another organisation. This enables other organisations to use your data, and the data will be provided free of charge.

If your personal data concerns more than your own data, we must consider whether providing the data would prejudice the rights of any third parties.

We will respond to your request for data portability within one month, however this can be extended by two months where the request is complex, or we receive a number of requests. We will inform you within one month of the receipt of the request and explain why the extension is necessary.

We may also request a reasonable fee or refuse to comply with your request for restriction if we consider it is manifestly unfounded or excessive. We will write to you within one month of receipt of your request and explain our decision. Any fee will be based on the administrative costs of complying with the request. If we charge a fee, then your request will not be processed until the fee is received.

Where we are not acting in response to a request, we will explain why and inform you of your right to an internal review, and thereafter to complain to the Data Commissioner's Office (ICO) within one month of receipt.

Right to Object

Individuals have the right to object to:

- The processing of your personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- The processing of their personal data for direct marketing (including profiling).

- The processing of their personal data for the purposes of scientific/historical research and statistics.

We will stop processing your personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual, or
- the processing is for the establishment, exercise or defence of legal claims.

We will inform you of your right to object at the point of first communication and in our Privacy Notice.

If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

We may also request a reasonable fee or refuse to comply with your request for restriction if we consider it is manifestly unfounded or excessive. We will write to you within one month of receipt of your request and explain our decision. Any fee will be based on the administrative costs of complying with the request. If we charge a fee, then your request will not be processed until the fee is received.

Where we are not acting in response to a request, we will explain why and inform you of your right to complain to an internal review, and thereafter, to complain to the Data Commissioner's Office (ICO) within one month of receipt.

Rights relating to Automated Decision Making

Automated individual decision making, and profiling is a decision made by automated means without any human involvement.

Examples of where an organisation may use this includes:

- An online decision to award a loan and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

The new data protection law will restrict organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

The restriction only covers solely automated individual decision-making that produces legal or similarly significant effects, although these effects are not defined, the decision must have a serious negative impact on an individual to be caught by this provision.

A legal effect is something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

We will only carry out solely automated decision making with legal or similarly significant effects if the decision is:

- Necessary for entering into or performance of a contract between an organisation and the individual.
- Authorised by law (for example, for the purposes of fraud or tax evasion).
- Based on the individual's explicit consent.
- The processing is necessary for reasons of substantial public interest.

We may also request a reasonable fee or refuse to comply with your request for restriction if we consider it is manifestly unfounded or excessive. We will write to you within one month of receipt of your request and explain our decision. Any fee will be based on the administrative costs of complying with the request. If we charge a fee, then your request will not be processed until the fee is received.

Where we are not acting in response to a request, we will explain why and inform you of your right to an internal review, and thereafter, to complain to the Data Commissioner's Office (ICO) within one month of receipt.

16) Restrictions on Data Rights

When dealing with your data rights request, a data controller or processor can restrict your rights if they consider it necessary to safeguard:

- National security.
- Defence.
- Public security.
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
- Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security.
- The protection of judicial independence and judicial proceedings.
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.
- A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority.
- The protection of the data subject or the rights and freedoms of others.
- The enforcement of civil law claims.

If we do place a restriction, then we will advise you of this, unless we believe by doing so would undermine the purpose for the restriction.

Where we are not acting in response to a request, we will explain why and inform you of your right to complain to the Data Commissioner's Office (ICO) and to a judicial remedy without undue delay and at the latest within one month.

17) Right to withdraw Consent

You have a right to withdraw your consent to the processing of your personal data by the OPCC at any time, if the lawful basis on which we processed that personal data was based on your consent. You can withdraw your consent easily at any time by contacting us directly via telephone, email, or by post using the details at the end of this Privacy Notice. The OPCC will thereafter inform you of what information we require from you, for us to withdraw your consent.

18) Data Protection Officer/OPCC contact details

The OPCC is a public authority and therefore it is mandatory for us to have an allocated Data Protection Officer, in compliance with Article 37 UK GDPR.

The Data Protection Officer (DPO) is accountable to the Chief Operating Officer of the OPCC and is responsible for reporting risks and recommending appropriate actions or opportunities in relation to the OPCC's processing of personal data and data protection as a whole.

You can contact the OPCC's Data Protection Officer in relation to any concerns you have with the OPCC's processing of your personal data, including exercising any of your individual rights or making a complaint.

E-mail: PCCOffice@Derbyshire.PNN.Police.UK

By post:
Data Protection Officer for the Police and Crime Commissioner
Office for Derbyshire
Butterley Hall
Ripley
Derbyshire DE5
3RS

By phone: 03001226003

19) Right to lodge a complaint with the ICO

If you are concerned about the way we have handled your personal data, you have the right to make a complaint to the Data Commissioners Office (ICO).

You can contact the ICO using the following contact details:

Address:

Data Commissioner's Office,

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire

SK9 5AF

E-mail: casework@ico.org.uk

Tel: 0303 123 1113

Website: https://ico.org.uk/

20) Transfers of personal data abroad

The OPCC will not normally transfer your data outside the European Economic Area ("EEA"). However, if this is required at any time, any personal data transferred to countries or territories outside the EEA will only be placed on systems complying with measures giving equivalent protection of personal rights, either through international agreements or contracts approved by the European Union.

21) Further processing

If the OPCC wishes to use your personal data for a new purpose not covered by this Privacy Notice, then the OPCC will provide you with a new privacy notice explaining this new use prior to commencing the processing. The new Privacy Notice will set out the relevant purposes and processing conditions. Where necessary, the OPCC will seek your explicit consent to the new processing.

22) Automated decision making and Profiling

Automated decision-making is the process of making a decision by automated means without any human involvement (i.e., a credit search). Profiling analyses aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them. Currently, the OPCC does not carry out any automated decision making or profiling on individuals.

23) Children's personal data

We do not provide services directly to children or proactively collect children's personal data. However, we are sometimes given data about children while handling a complaint, conducting an appeal or providing a service to the public.

The data in the relevant parts of this privacy notice applies to children as well as adults.

The length of time that we keep children's personal data depends upon our reasons for collecting it and any legislation that may govern our retention periods.

For more data about how long we hold personal data and see our retention schedule on our policies page on our website or please contact the OPCC via the data at the end of this notice.

24) Service adjustments/Equalities Act 2010

As a public authority and a provider of services to the public, we have a legal duty to comply with the Equality Act (2010).

This means we need to make service adjustments for anyone with a disability who contacts us in any capacity, to eliminate any barriers to accessing our services. Our lawful basis for processing this data is legal obligation - under Article 6(1)(c) of the GDPR, as we have a legal obligation to provide this service to you under the Equalities Act 2010.

Our processing of your Special Category Data (such as health data) will be based on Article 9(2)(a) UK GDPR, which means we need your explicit consent to process this data.

We will create a record of your reasonable adjustment requirements. This will include your name, contact details and type of adjustment required, along with a brief description of why it is required. Relevant staff in the OPCC will then be able to access this data to ensure they are communicating with you in the required way.

The length of time that we keep this personal data depends upon our reasons for collecting it and any legislation that may govern our retention periods.

For more data about how long we hold personal data and see our retention schedule on our policies page on our website or please contact the OPCC via the data at the end of this notice.

25) Restricted contact

We may impose a restriction on your access to our services if it is necessary to protect our staff from unacceptable behaviour, as defined in our policy for dealing with unreasonable and unreasonably persistent complainants and vexatious complaints.

The lawful basis we rely on to process your personal data is public task – under Article 6(1)(e) UK GDPR, which allows us to process personal data when this is necessary to perform our public tasks as a public authority.

If we do this, we will explain to you the restriction we have applied and why we feel it is necessary. We will create a record of the restriction for administration purposes, so OPCC staff members know the restrictions are in place. This will include your name, contact details and a description of why we have imposed a restriction/s.

The decision to impose a restriction/s will be taken, and reviewed, by a senior manager in the OPCC (normally the Chief Operating Officer). We will write to you

explaining why we have applied the restriction. We will review the restriction periodically, and we may remove the restriction if we feel this is appropriate.

The length of time that we keep personal data depends upon our reasons for collecting it and any legislation that may govern our retention periods.

For more data about how long we hold personal data and see our retention schedule on our policies page on our website or please contact the OPCC via the data at the end of this notice.

26) Single point of contact

We may provide a single point of contact if we believe that this is the most appropriate way in which to communicate with you.

The lawful basis we rely on to process your personal data is public task – under Article 6(1)(e) UK GDPR, which allows us to process personal data when this is necessary to perform our public tasks as a public authority.

A decision will be made by a senior member of management (normally the Chief Operating Officer of the OPCC) to give you a single point of contact. This may be where you have several complaints, and we believe it will be more efficient for us to deal with them via a single point of contact in the OPCC.

We will make a record of the fact that you have a single point of contact, and all relevant OPCC staff will be aware of this to enable us to manage communications with you. It will include your name, contact details and a description of the need to have a single point of contact. We will review this requirement from time to time to ensure it is still the most effective manner in which to communicate with you.

The length of time that we keep this personal data depends upon our reasons for collecting it and any legislation that may govern our retention periods.

For more data about how long we hold personal data and see our retention schedule on our policies page on our website or please contact the OPCC via the data at the end of this notice.

27) How we keep your personal data safe

The OPCC takes the security of all personal data under our control very seriously, and we will comply with all relevant parts of data protection legislation and law relating to security.

We will ensure that appropriate training, policies, technical and procedural measures are in place to secure personal data. These will include, but are not limited to, ensuring our buildings are secure and protected by adequate physical means, and that our systems meet appropriate industry and government security standards.

28) Changes to this notice

This privacy notice will be updated every three years, unless changes in legislation, laws or internal processes dictates otherwise.

END