

## **Durham Constabulary Safeguards Pledge for Processing of Special Categories of Personal Data v1-0**

Under the Data Protection Act 2018 (DPA) the Chief Constable of Durham Constabulary is required to have an appropriate policy document and additional safeguards in place when relying on certain conditions to carry out the processing of special categories of personal data and criminal conviction data.

This document is our safeguard pledge which explains our policies and procedures in relation to the processing of special categories of personal data in reliance on specific conditions in Schedule 1 of the DPA. This pledge complements our [privacy notice and workforce privacy notice](#).

Durham Constabulary is determined by the DPA as Competent Authority to process sensitive personal data under Part 3 for the purposes of law enforcement. The policies and procedures in relation to this processing are covered by the [Durham Constabulary Safeguards Pledge for Sensitive Processing of Personal Data for law enforcement purpose](#).

### **Special Categories of Data**

Special categories of personal data is defined at Article 9 GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

### **Criminal Conviction Data**

There may be occasions when criminal convictions and offence data will be processed under the GDPR and not under Part 3 Law Enforcement.

### **Conditions for Processing Special Category and Criminal Offence Data**

The most common GDPR Articles we process personal data under include:

Article 9(2) (b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Chief Constable or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences, medical history, complaints of conduct and political activity declarations.

Article 9 (2) (g) - reasons of substantial public interest. The Chief Constable has statutory responsibilities as defined in UK law. The role of the Chief Constable of Durham is to provide an efficient and effective police force, protect the public and to prevent and detect crime. As a public authority processing of personal data is often for the purposes of substantial public interest and is necessary for carrying out our role.

Examples of processing includes information we process in relation to the disclosure of personal data for safeguarding purposes, conduct matters, fitness for duty or employment that may fall out of statutory obligations for employment.

Article 9 (2) (j) – for archiving purposes in the public interest.

An example of our processing is the archiving of records which are in the public interest. Although the police service does not have a specific obligation under the Public Records Act 1958, records will be retained to meet potential obligations under the Inquiries Act 2005 and in line with national police guidelines.

Article 9 (2) (f) – for the establishment, exercise or defence of legal claims.

Our processing will include processing data relating to employment tribunal, judicial review or other litigation.

Article 9 (2) (c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of processing would be accessing and sharing a member of staff's health information in a medical emergency.

We process criminal offence data under Article 10 of the GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an officer or employee or in line with contractual obligations.

### **Processing which requires an Appropriate Policy Document**

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an appropriate policy document.

This pledge demonstrates that the processing of special categories of personal data and criminal offence data based on the specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles and Schedule 1 Part 4 of the DPA.

### **The Data we Process**

Durham Constabulary processes special category data about members of the work force. The processing is necessary to fulfil our obligations as an employer and public authority. This includes information about health and wellbeing, ethnicity, photographs and their membership of any trade union. Further information about this processing can be found in our workforce privacy notice.

Our processing for reasons of substantial public interest relates to the data we process in order to fulfil our statutory function as a public service. This may be information to help safeguard individuals or to ensure the efficient and effective use of public funds.

In the performance of our public task we may process criminal conviction data outside of the law enforcement purpose to protect and safeguard the public.

### **Schedule 1 Conditions for Processing**

The following are the most common conditions Durham Constabulary will process special categories of data under Part 1 of Schedule 1:

- **Paragraph 1(1)** employment, social security and social protection.

The following are the most common conditions Durham Constabulary will process special categories of data under Part 2 of Schedule 1 – substantial public interest:

- **Paragraph 6 (1) and (2)(a) (b)** - statutory etc
- **Paragraph 8** - equality of opportunity or treatment
- **Paragraph 10 (1)** - preventing or detecting unlawful acts
- **Paragraph 11 (1) and (2)** - protecting the public against dishonesty
- **Paragraph 12 (1) and (2)** - regulatory requirements relating to unlawful acts and dishonesty
- **Paragraph 15** - suspicion of terrorist financing and money laundering
- **Paragraph 17** - counselling etc
- **Paragraph 18** - safeguarding of children and of individuals at risk
- **Paragraph 21** - occupational pensions
- **Paragraph 24 (1) and (2)** - disclosure to elected representatives
- **Paragraph 25** - informing elected representatives about prisoners
- **Paragraph 26** - publication of legal judgments

### **Criminal Offence Data**

The most common conditions we process criminal offence data for in Parts 1 and 2 of Schedule 1:

- **Paragraph 1** - employment, social security and social protection
- **Paragraph 6 (2) (a)** - statutory, etc. purposes
- **Paragraph 10** – preventing or detecting unlawful acts
- **Paragraph 11** – protecting the public against dishonesty etc.
- **Paragraph 18** - safeguarding of children and individuals at risk
- **Paragraph 24** - disclosure to elected representatives
- **Paragraph 26** - publication of legal judgments

## **How we will meet the principles for processing in reliance on specific conditions**

### **Lawful, Fair and Transparent**

Durham Constabulary will undertake processing in reliance on specific conditions where there is a lawful basis to do so.

We will communicate fair processing information to individuals through the Durham Constabulary website. Wherever possible on request we will also make the same information available to individuals by other methods.

We will communicate processing to members of the constabulary and other relevant individuals who carry out tasks on behalf of the constabulary by way of a workforce privacy notice which will be made available through appropriate methods. Where appropriate it may be necessary to inform individuals of certain data processing on a case by case basis and this will form part of organisational policy, procedure and process.

### **Specified Purpose**

We will process personal data for purposes as explained above, the processing will be necessary and proportionate to that purpose and will undertake steps to ensure compatibility assessments are carried out to establish that any further processing is lawful.

We may share data with another controller and this will only take place when authorised by law to do so.

We may undertake joint controller status with other controllers.

### **Data Minimisation**

Any personal data collected will be limited to that which is necessary for the purposes of processing. Where it is identified that personal data obtained or provided is excessive to the purpose, we will review and take steps to erase or if not possible take measures to minimise further processing.

### **Accuracy**

We will ensure as far as possible that the data we hold is accurate and kept up to date. Officers and employees of the Constabulary will undertake amendments or augmentation of personal data when it is appropriate to do so.

Where it is identified and verified that any personal data which is held is inaccurate, we will take every reasonable step to erase or rectify without delay. If it is not possible to erase or rectify we will take steps to minimise further processing. Where a lawful basis exists to continue processing data we may conclude to retain or not take steps to rectify the data. In the cases where this is identified the decision will be documented.

### **Storage Limitation**

Special categories of data processed by us will be retained in line with local and national retention guidance and where applicable, we seek to comply with the Authorised Professional Practice for the

Management of Police Information. The determination of the retention periods is based on national guidance, legal obligations and the necessity of its retention for our business needs.

In cases where it is not possible to delete or dispose in accordance with policies, for example system constraints, we endeavour to identify and apply measures to limit further processing.

### **Integrity and Confidentiality (Security)**

Electronic information is processed within our secure network. Physical records containing personal information are subject to handling conditions and security measures are applied when transportation of such documents is required. Employees with access to personal data undergo vetting and vetting reviews during employment and access controls are applied to limit access to those that require it. Audit functionality is deployed across systems which logs transactions such as creation, access, alteration and deletion.

Where suppliers are required to process data on our behalf appropriate processing agreements are put in place.

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

May 2020