

**Appropriate Policy document**

**Processing of special categories of personal data and criminal offence data (not Law Enforcement processing).**

Police and Crime Commissioners were established under the Police Reform and Social Responsibility Act 2011.

The Data Protection officer can be contacted at:

Office of the PCC, Andy Hocking House, Alderson Drive, Exeter, EX2 7RP

Email: opcc@dc.police.uk.

Tel: 01392 225555

**What this policy does**

This policy explains the procedures for securing compliance with the data protection principles listed below in relation to the processing of special categories of personal data and criminal conviction etc. data. It also explains the retention and erasure policies in relation to that data.

**Special category data**

Special category 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.

Article 9(1) of the GDPR prohibits the processing of special categories of personal data unless a specific condition in Article 9(2) is met, as well as there being a valid legal basis under Article 6 for the processing. In addition, a condition in the Data Protection Act 2018, Schedule 1 parts 1 or 2 may also need to be met, and an Appropriate Policy Document in place.

**Criminal offence data**

Article 10 of the GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the Data Protection Act 2018 includes in this definition personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as ‘criminal offence data’.

Processing of criminal offence data requires a lawful basis under Article 6 of the GDPR and that the data is processed in an official capacity, or a condition in the Data Protection Act 2018, Schedule 1 parts 1, 2 or 3 must be met.

**Requirement for an appropriate policy document**

Most of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document in place, setting out and explaining our procedures for ensuring compliance with the Data Protection principles in Article 5 of the GDPR and policies regarding the retention and erasure of such personal data. This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the Data Protection Act 2018.

In addition it provides some further information about our processing of special category and criminal offence data where a policy document isn’t a specific requirement.

**Processing of special category and criminal conviction data for law enforcement purposes**

We do not process special category and criminal offence data for law enforcement purposes, however where necessary, we may share criminal offence data with other authorities for processing for law enforcement purposes in their capacity as a competent authority (as defined in the Data Protection Act 2018). This processing falls under Part 3 of the Data Protection Act 2018. In general, the competent authorities that we may share special category and criminal offence data with will be the Devon and Cornwall Police, or another police force as appropriate, and the Office for Police Misconduct. For further information about how they process this data, please see their appropriate policy documents:

* Devon and Cornwall Police [Appropriate Policy Document](https://www.devon-cornwall.police.uk/media/971714/appropriate_policy_law_enforcement_dc_police.pdf) Sensitive Processing for Law Enforcement Purposes September 2019
* Independent Office for Police Misconduct [appropriate policy document](https://www.policeconduct.gov.uk/sites/default/files/Documents/Who-we-are/Our-Policies/Appropriate_Policy_Document_Core_Functions.pdf) for Processing special category and criminal offence data for the purposes of investigations, appeals and our other core functions

**The lawful bases for processing (Article 6 conditions)**

We process special category and criminal offence data under one or more the following lawful bases under Article 6 of the GDPR.

(a) Consent: where the data subject has given us clear, explicit and unambiguous consent for you to process their personal data for a specific purpose.

(b) Contract: where the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: where the processing is necessary for us to comply with the law (but not including contractual obligations).

(d) Vital interests: where the processing is necessary to protect someone’s life.

(e) Public task: where the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: where the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (We will not use this basis when we are processing data to perform our official tasks.)

**Conditions for processing special category and criminal offence data (Article 9 Article 10 and Schedule 1 conditions).**

We process special categories of personal data under the following GDPR Articles:

* Article 9(2)(a) – the data subject has given their explicit consent to the processing of the personal data for one or more specified purposes;

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our customers who require a reasonable adjustment to access our services.

* 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 us or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences, political activity declarations, and reasonable adjustments.

* 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 our processing would be using health information about a member of staff in a medical emergency.

* Article 9(2) (e) – the data subject has already made the personal data public.

Where the data subject has themselves put their personal data into the public domain, for example, on their own social media account.

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

Examples of our processing include processing relating to any employment tribunal or other litigation.

* Article 9(2)(g) - reasons of substantial public interest.

Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role. Substantial public interest conditions are set out in Schedule 1 of the Data Protection Act 2018 part 2.

Examples of our processing in the substantial public interest include:

* Elected representatives responding to requests

An example is where the police and crime commissioner or a person acting with their authority responds to enquiries and correspondence.

* Disclosure to elected representatives.

An example is where the data subject discloses special category personal data relevant to a police service complaint about hate crime at a ‘meet your PCC’ event.

* Preventing or detecting unlawful acts.

An example would be where a data subject discloses special category data in an allegation of an unlawful act about a Chief Constable, and in order for us to progress the complaint we need to process the data in preparation for disclosure to the competent authority to investigate.

* Protecting the public against dishonesty etc.

An example is where we administrate police misconduct processes.

* Regulatory requirements relating to unlawful acts and dishonesty etc.

An example is where we administrate police misconduct processes.

* Safeguarding of children and of individuals at risk

An example is where a data subject discloses concerns about an individual who they believe is at risk at a community engagement event.

* Safeguarding of economic well-being of certain individuals

An example is where a data subject discloses concerns about an individual who they believe is at risk at a community engagement event.

* Equality of opportunity or treatment.

An example is where we collect and process special category data of applicants for jobs to ensure that our recruitment processes are attracting candidates from diverse communities, and providing equality of access.

* Racial and ethnic diversity at senior levels of organisations

An example is where we collect and process special category data of applicants for jobs, but also from post holders to promote and maintain diversity in our organisation.

* Article 9(2)(j) – for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – statistical purposes.

An example of our processing is for the scrutiny of police performance.

In relation to processing special category data under Articles (2)(b), and (j), we also rely on the conditions and safeguards in Schedule 1 Part 1 of the Data Protection Act 2018 (Employment, social security and social protection).

We process criminal offence data under Article 10 of the GDPR and the following conditions in Schedule 1, part 1 and 2 of the Data Protection Act 2018.

Part 1 conditions

* Employment, social security and social protection

An example is when we process criminal offence data when carrying out pre-employment suitability checks and declarations by an employee in line with contractual obligations.

Part 2 conditions

* Elected representatives responding to requests

An example is where the police and crime commissioner or a person acting with their authority responds to enquiries and correspondence that contain allegations of criminal conduct.

* Disclosure to elected representatives.

An example is where the data subject discloses criminal offence data relevant to a police service complaint at a ‘meet your PCC’ event.

* Preventing or detecting unlawful acts.

An example is where the data subject discloses allegations of an unlawful act in a complaint, and in order for us to progress the complaint we need to process the data in preparation for disclosure to competent authority to investigate.

* Protecting the public against dishonesty etc.

An example is where we administrate police misconduct processes, and review the handling of police complaints.

* Regulatory requirements relating to unlawful acts and dishonesty etc.

An example is where we administrate police misconduct processes, and review the handling of police complaints.

* Safeguarding of children and of individuals at risk

An example is where a data subject discloses concerns about an individual who they believe is at risk of a criminal act against them at a community engagement event.

* Safeguarding of economic well-being of certain individuals

An example is where a data subject discloses concerns about an individual who they believe is at risk of a criminal act against them at a community engagement event.

**The OPCCs compliance with the requirements of the GDPR Article 5 principles in its processing of special category and criminal offence data**

**Record of processing**

We maintain a record of our processing activities in accordance with Article 30 of the GDPR.

**Accountability principle**

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

* The appointment of a data protection officer who reports directly to our highest management level.
* Taking a ‘data protection by design and default’ approach to our activities.
* Maintaining documentation of our processing activities.
* Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
* Implementing appropriate security measures in relation to the personal data we process.
* Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

**Principle (a): lawfulness, fairness and transparency**

We provide clear and transparent information about why we process personal data including our lawful basis for processing using a range of methods, for example in this policy document, in privacy notices published on our website, when acknowledging correspondence, verbally and by request.

We publish our record of processing activities on our website.

Where we are relying on explicit consent for the processing of personal data this will be an affirmative action. More information about [consent](https://www.devonandcornwall-pcc.gov.uk/information-hub/freedom-of-information/data-protection/) can be found here.

**Principle (b): purpose limitation**

Our privacy notices detail the purposes for which the personal data are processed.

Processing of personal data will be restricted to only that which is necessary for the relevant purpose and it will not be used for a matter which is incompatible with that purpose, unless an exemption in accordance with Schedule 2, Part 1 of the GDPR applies.

If it is considered that further processing should be carried out (and that further processing is not based on consent), and the purpose does not fall within Schedule 2 Part 1 of the Data Protection Act 2018 (exemptions etc. from the GDPR), action will be taken as per Article 6(4) of the GDPR (requirements where processing for another purpose) to determine compatibility or otherwise of the proposed processing.

If it is decided that the further processing is not incompatible with the original purpose, action will be taken as per Article 13(3) or Article 14(4) (requirement to provide information to the data subject on the processing) unless it is not appropriate, as per Article 13(4) or 14(5) respectively.

**Principle (c): data minimisation**

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

**Principle (d): accuracy**

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don’t apply, we will document our decision.

**Principle (e): storage limitation**

All special category data processed by us for the purposes detailed above are, unless retained longer for archiving purposes, retained for the periods set out in our [retention schedule](../../Records%20management/RMT_POL_File-Retention.pdf). We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

**Principle (f): integrity and confidentiality (security)**

Electronic information is processed within the police secure network. Devon and Cornwall Police applies the information security standards set for the National Policing Community by the Cabinet Office and the Home Office. This includes encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password controlled access, technical assurance and technical audits and end point management.

Hard copy information is processed in line with our security procedures.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

All staff are required to undertake mandatory data protection training. Anyone who works on our behalf who has access to our systems and information is required to be security vetted prior to being given access to our information, systems, and are trained on them before access is granted.

Our building is kept physically secure with access only being granted to individuals who are authorised to access.

Further measures include the following Policies:

• Data Protection Policy.

• Information Security Policy and Procedure.

• Physical Security Policy.

**Retention and erasure policies**

Our retention and erasure practices are set out in our [retention schedule](https://devonandcornwall.s3.amazonaws.com/Documents/Our%20information/Policies%20of%20the%20OPCC/RMT_POL_File-Retention.pdf).

Requests for erasure of personal data will be dealt with in accordance with Article 17 of the GDPR and when relevant, recipients of the relevant data will be notified of the erasure, in accordance with Article 19 of the GDPR unless this proves impossible or involves disproportionate effort. Any such decision will be recorded.

**Appropriate Policy Document Review Date**

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

This policy will be reviewed annually or revised more frequently if necessary.

**Additional special category processing**

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our [privacy notices](https://www.devonandcornwall-pcc.gov.uk/information-hub/freedom-of-information/data-protection/) and our record of processing activity.

**Date of policy: November 2019**