

APPROPRIATE POLICY DOCUMENT

July 2020

**Office of the Police and Crime
Commissioner for Warwickshire**



**Philip Secombe
Police and Crime
Commissioner
for Warwickshire**

Policy/Procedure Title	Appropriate Policy Document
Responsible Party	Chief Executive

Security Classification	Public
Disclosable under Freedom of Information Act 2000	Yes

Policy Implementation Date	01 July 2020
Next Review Date Prior To	01 July 2021

Revision record

Date	Nature of revision
1.0 Month YYYY	n/a

Introduction

This Policy Document sets out details of the Office of the Police and Crime Commissioner for Warwickshire's (OPCC) processing of special categories of personal data and criminal offence data.

As part of the Police and Crime Commissioner's statutory functions pursuant to the Police Reform and Social Responsibility Act 2011, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

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.

Criminal conviction data

Article 10 GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes 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'.

This policy document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 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 DPA 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. The information supplements our [privacy notice](#) and staff privacy notice (available upon request).

Conditions for processing special category and criminal offence data

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

- i. 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 PCC or the data subject in connection with employment, social security or social protection.

Examples of our processing include monitoring and managing staff sickness absence and administering benefits such as statutory maternity pay.

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

The Police and Crime Commissioner (PCC) is a public authority and has certain powers and obligations pursuant to the Police Reform & Social Responsibility Act 2011. The PCC for Warwickshire is statutorily required to secure the maintenance of the police force for Warwickshire and to secure that the police force is efficient and effective.

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.

Examples of our processing include the information we seek or receive as part of investigating a complaint against the Chief Constable.

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

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

An example of our processing is the transfers we make to the National Archives as part of our obligations as a public body under the Public Records Act 1958.

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

Examples of our processing include processing relating to any Police Appeals Tribunal or other litigation.

v. Article 9(2)(a) – explicit consent

In the limited circumstances where we may 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.

vi. 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.

We process criminal offence data under Article 10 of the GDPR

Examples of our processing of criminal offence data include pre-employment police vetting checks.

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 APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the OPCC. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union. Further information about this processing can be found in our staff privacy notice (available upon request).

Our processing for reasons of substantial public interest relates to the data we receive or obtain in order to fulfil our statutory functions. This may be information provided to us as part of a

complaint against the Chief Constable. Further information about this processing can be found in our [privacy notice](#).

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

Schedule 1 conditions for processing

Special category data

We process special category data for the following purposes in Part 1 of Schedule 1:

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

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- **Paragraph 6(1) and (2)(a)** statutory, etc. purposes
- **Paragraph 8(1)** equality of opportunity or treatment
- **Paragraph 23(1) and (2)** elected representative responding to requests
- **Paragraph 24(1) and (2)** disclosure to elected representatives

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1** – employment, social security and social protection
- **Paragraph 6(2)(a)** – statutory, etc. purposes

Securing compliance with the Data Protection principles (GDPR Article 5)

In summary the principles set out in Article 5 of the GDPR are as follows:

Principle (a): lawfulness, fairness and transparency

Principle (b): purpose limitation

Principle (c): data minimisation

Principle (d): accuracy

Principle (e): storage limitation

Principle (f): integrity and confidentiality (security)

In addition, Article 5 requires that the data controller is responsible for and can demonstrate compliance with the above principles (the accountability principle)

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing (in compliance with GDPR articles 6 and 9) in our privacy notice, staff privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary for the exercise of functions conferred on the PCC pursuant to the Police Reform and Social Responsibility Act 2011.

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the OPCC in its capacity as a public authority e.g. the Equality Act.

Principle (b): purpose limitation

We process personal data for purposes of substantial public interest as explained above when the processing is necessary for us to fulfil our statutory functions, to comply with obligations under equalities legislation, for responding to requests or for disclosures to elected representatives.

We are authorised by law to process personal data for these purposes. We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose. We have in place an information sharing agreement template and procedure (available upon request), based upon the ICO's data sharing statutory code of practice, which sets out good practice principles of information sharing with other data controllers.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

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. We have in place a data protection impact assessment procedure (DPIA) (available upon request) and conduct DPIAs for high risk processing to ensure that any data that is processed is adequate for fulfilling our statutory requirements but not excessive for our needs.

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 purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our records management and retention policy (available upon request). The retention period for data is based on our legal obligations and the necessity of its retention for our business needs. Our retention policy is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within a secure ICT network provided by Warwickshire police force and we have adopted relevant police force ICT policies and procedures.

Hard copy information and electronic information is protectively marked in accordance with the government security classification scheme.

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

We have in place mandatory training for staff in the secure handling of information which includes refresher training and briefing sessions. We have a mandatory information security

incident reporting procedure (available upon request) in place and staff are trained in the identification, containment and management of any breach of information, should this occur.

All our staff and volunteers are required to be police vetted in line with non-police personnel vetting requirements.

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. Our data protection officer is Warwickshire Legal Services who can be contacted via email at: wls@warwickshire.gov.uk.
- Maintaining a record of our processing activities (ROPA).
- 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 policies and procedures and update or amend them when required.

Retention and erasure policies

Our retention and erasure practices are set out in our records management and retention policy (available upon request).

APD 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 notice](#) and staff privacy notice (available upon request).