Appropriate Policy Document
Processing of Special Categories of Personal Data and Criminal Convictions Data (Non-Law Enforcement Processing)

Wiltshire Police (WP) is a police force established under the Police Act 1996. The Data Protection Team can be contacted at:

Devizes HQ, London Road, Devizes, SN10 2DN.

DataProtectionOfficer@wiltshire.pnn.police.uk

What this Policy does

This policy explains WP 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. This policy is a requirement under Part 4 of Schedule 1 of the Data Protection Act 2018 (DPA).

Special categories of personal data are:

- 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 an individual's sexual behaviour or sexual orientation.

Criminal conviction data

Criminal conviction data also includes processing in relation to offences or related security measures.

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. In addition a condition in the DPA, Schedule 1 Parts 1 or 2 must also be met.

The WP Privacy Notice sets out the legal basis for processing the personal data held under both Articles 6 and 9 and the relevant Schedule 1 conditions.

Processing of personal data relating to criminal convictions etc data

As an official authority processing personal data in accordance with Article 6 of the GDPR, WP meets the requirements of GDPR Article 10 for the processing of personal data relating to criminal convictions etc data. There may be occasions where personal data regarding convictions or alleged offences will not be processed for our law enforcement purposes. (For example for recruitment and vetting purposes where an employee may have existing convictions or offences not dealt with by WP.)

The Data Protection Principles

The principles set out in the GDPR require personal data to be:

1. Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

2. Collected for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation)

3. Adequate, relevant and not excessive in relation to the purposes for which they are processed (data minimisation)

4. Accurate and where necessary kept up to date (accuracy)

5. Kept in a form which permits identification for no longer than is necessary for the purposes for which the data are processed (storage limitation)

6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical and organisational measures (integrity and confidentiality).

In addition the controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle).

How we will meet these principles in relation to special categories of personal data:

Principle 1. Lawful, fair and transparent

WP will communicate fair and transparent processing information to individuals using a through the provision of privacy notices, at the time the information is provided to us by the data subject.

The privacy notices are also on the WP Website, available by contacting the Data Protection Team and in other formats if required. These notices detail the legal basis for processing types of personal data.

Where explicit consent is requested or given from an individual to allow processing of personal data this will be an affirmative action. The individual will be provided with details of what personal data are involved, what processing they are consenting to, what will happen to their data (e.g. where will it be stored, will it be shared etc.), and the length of time the data will be retained. They will also be advised of their right to withdraw consent at any time. Where consent is requested or given, this information and the response from the individual will be documented and available for an audit trail.

Principle 2. Specified, explicit and legitimate purposes

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

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, action will be taken as per Article 6(4) of the GDPR to determine compatibility or otherwise of the proposed process. The result of this will be documented with the reasons for the decision.

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) unless it is not appropriate, as per Article 13(4) or 14(5) respectively.

Principle 3. Adequate, relevant and not excessive

Any personal data collected for general processing purposes will be restricted to that which is necessary for the purposes of processing. The data protection training undertaken by all officers and staff emphasises that police records must ensure that personal data is adequate, relevant, unambiguous and professionally worded. Matters of opinion, which are not fact, will be clearly recorded as such.

Principle 4. Accurate and where necessary kept up to date

We will ensure as far as possible that the personal data we process are accurate and kept up to date. In some circumstances we may need to retain factually inaccurate information e.g. information provided by a 3rd party which does not represent the true facts.

All officers and staff are made aware of the need for accuracy and are responsible for the accuracy of the personal data they process. Checks are carried out on the accuracy of data during audits and line manager checks.

Personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible at present due to the limitations of IT systems, there will be an addendum to that personal data advising of the inaccuracy. When relevant, the processing will be restricted in accordance with Article 18 of the GDPR.

Recipients of the relevant data will be notified of the erasure, rectification or restriction in accordance with Article 19 of the GDPR unless this proves impossible or involves disproportionate effort.

Principle 5. Kept for no longer than is necessary

WP has a Records Management, Retention and Disposal Schedule which outlines the principles which WP adhere to for the retention, review and disposal of records which have been created within its activities and functions. This Policy is available on WP's website or can be provided by request to the Records Management Team.

When an individual withdraws consent to the processing of personal data (where consent has been relied upon for the lawful basis), that data will be destroyed on receipt of the withdrawal unless there is an overriding purpose for continued processing.

Principle 6. Appropriate security

WP has developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of all personal data processed.

Technical measures - WP 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.

Organisational measures - All officers and staff are required to undertake mandatory data protection training. All new staff, officers and contractors are vetted prior to being given access to WP information, systems and records.

Officers and staff receive training in how to use police systems before being granted access. Buildings are kept physically secure with access only being granted to individuals who are authorised to access.

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 has a direct reporting line 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.

Further measures include the following Policies:

- Data Protection Policy.
- Information Security Policy

Requests for erasure of special category personal data

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.

Retention and review of this policy

This policy document will be retained in accordance with Part 4 of Schedule 1 of the DPA. It will be made available to the ICO on request.

The policy will be reviewed on an annual basis (or more regularly if circumstances require it) and updated as necessary at these reviews.