Data Protection Policy

POLICY STATEMENT.

Wiltshire Police and the Office of Police and Crime Commissioner (OPCC) have a statutory obligation to process personal data in accordance with the provisions of the UK General Data Protection Regulation (UKGDPR) in respect of non law enforcement processing and the Data Protection Act 2018 (DPA 2018) in respect of law enforcement processing. For ease of reference these will be collectively referred to as 'Data Protection legislation' for the remainder of this document.

Wiltshire Police and the Office of Police and Crime Commissioner (OPCC) have a statutory obligation to process personal data in accordance with the provisions of the UK General Data Protection Regulation (UKGDPR) in respect of non law enforcement processing and the Data Protection Act 2018 (DPA 2018) in respect of law enforcement processing. For ease of reference these will be collectively referred to as 'Data Protection legislation' for the remainder of this document.

The DPA 2018 supplements the UK General Data Protection Regulations (UKGDPR). Accordingly, the DPA 2018 ensures a single, coherent, domestic regime for the processing of personal data for law enforcement purposes.

In order to fulfil its statutory obligations, Wiltshire Police and the OPCC has implemented the provisions of the DPA 2018 in all respects, and follows the guidance contained in the College of Policing APP, the NPCC Data Protection Manual of Guidance and ICO guides.

This policy applies to individuals at all levels of both organisations including Police Officers, Police and OPCC Staff, Special Constabulary, PCSOs, temporary staff and 3rd parties (for example but not necessarily limited to partner agency staff, consultants, contractors and volunteers) who have authorised access to personal data as part of their role.

All Wiltshire Police officers, police and OPCC staff and 3rd parties must have a clear understanding of their personal responsibilities under the data protection legislation and how this affects the processing of personal data.

Wiltshire Police and the OPCC will take criminal and/or disciplinary action against any category of person mentioned above who wilfully, without authority or a defined policing purpose or other statutory or business purpose, accesses and/or misuses personal data held by either the Force or OPCC. Any use of personal data that does not have a defined policing or other statutory or business purpose is likely to constitute a misuse.

For the purpose of this policy, 'data' and 'information' shall have the same meaning.

KEY DEFINITIONS.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, 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.

'Special Category Data' means racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of 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.

'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

ROLES AND RESPONSIBILITIES.

The Data Protection legislation identifies the following roles in respect of the processing of personal information:

The **Data Controller** – The person who determines the manner and purpose for which personal data is processed; The Chief Constable is the Data Controller for Wiltshire Police; the Police & Crime Commissioner for Wiltshire & Swindon is the Data Controller for the Office of the Police & Crime Commissioner.

The **Data Protection Officer (DPO)** - the person who assists the Force in advising and monitoring compliance, provides advice regarding Data Privacy Impact Assessments, and is the point of contact for the supervisory authority (in the UK this is the Information Commissioner's Office). The DPO is based within the Information Management and Assurance department.

All **Managers and Supervisors -** It is the responsibility of all Officers and Staff who have a supervisory role to ensure that their staff operate within the terms of the Data Protection Legislation and any associated Force policies and procedural guides. This must include regular checks of work to identify training and development needs in this area and to ensure that the quality of Force or OPCC information assets is of a high standard.

All **Officers, Staff and 3rd Parties -** There is a personal responsibility on all persons working for or on behalf of the Constabulary to ensure that they comply with the Data Protection Legislation, Force policy and/or procedural guides when undertaking their duties.

Data Processor – In relation to personal data means any third party (other than an employee of the data controller) who processes the data on behalf of the data controller. The UKGDPR places specific legal obligations on Data Processors. For example, Data

Processors are required to maintain records of personal data and processing activities and are liable legally if they are responsible for a breach. The Data Controller(s) must ensure that contracts with Data Processors comply with the UKGDPR.

REGISTRATION.

The Supervisory Authority for compliance with the Data Protection Legislation is the Information Commissioner. Wiltshire Police and the OPCC are required to register with the Information Commissioner's Office (ICO) and pay the appropriate fee. The Data Protection Officer is responsible for maintaining this process.

GENERAL PROCESSING – GDPR and Part 2 of the DPA 2018.

UKGDPR and Part 2 of the DPA 2018 relate to general processing and covers police and OPCC support functions such as Human Resources, Occupational Health, Finance and Payroll (including pensions), Estates, ICT and Procurement.

UKGDPR does **NOT** apply to the processing of personal data by Wiltshire Police (as a competent authority) for Law Enforcement purposes.

LAW ENFORCEMENT PROCESSING – Part 3 of the DPA 2018.

Part 3 of the DPA 2018 relates to the processing of personal data for a Law Enforcement Purpose; "**the purposes of 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.**"

RIGHTS OF THE DATA SUBJECT.

The Data Protection Legislation provides data subjects with a number of rights. If personal data is held by the Wiltshire Police for Law Enforcement purposes then the right to data portability and the right to object do not apply.

The individual rights are:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restrict processing
- Right to data portability*
- Right to object*
- Rights in relation to automated processing

The right of access is managed by the Force Disclosure Unit (FDU) who process all Right of Access Requests (ROARs) on behalf of Wiltshire Police in accordance with the Right of Access procedural guide. In the event that you or your department receive a Right of Access request, please forward the request expeditiously to the FDU (forcedisclosureunit@wiltshire.police.uk; for more information see: Verbal Subject Access Requests).

The right to rectification and the right to erasure are managed by the RRD Department in accordance with the Record Deletion, Amendment and Restriction Policy.

Data Subjects wishing to exercise any of the other rights should contact the DPO in the first instance; dataprotectionofficer@wiltshire.police.uk.

DATA BREACHES.

A 'personal data breach' means an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

All officers/staff are to familiarise themselves with the Data Breach Notification Procedure. It is vital that a potential data breach is notified to either the Force Data Protection Officer at the earliest opportunity, and within 72 hours.

PRIVACY BY DESIGN.

The completion of a Data Protection Impact Assessment (DPIA; screening questionnaire and/or full DPIA) will be undertaken for all new processes that involve the processing of personal data. Further advice can be obtained from the Data Protection Officer (DPO) dataprotectionofficer@wiltshire.police.uk and Information Security Officer (ISO).

INFORMATION SHARING.

Wiltshire Police and OPCC will share information, including personal information, where it is lawful and appropriate to do so.

Wiltshire Police and OPCC will not share information, including personal information, in support of revenue gathering processes by partners or other organisations.

Where regular sharing of information with a partner is considered necessary an Information Sharing Agreement (ISA) will be entered into. See the Information Sharing Policy for further information.

This does not prevent the urgent sharing of information where there is an overriding duty to the public, i.e. life threatening circumstances.

Information received from partners will be managed in accordance with the guidance on MoPI, specific information handling procedures or constraints on the use of information will be detailed within each individual ISA.

DATA PROCESSING.

Where a Processor is to be carrying out processing on behalf of Wiltshire Police or OPCC a Data Processing Contract will be implemented to ensure that all Article 28 (UKGDPR) obligations are met. Any Data Processing Contract must be reviewed by the Data Protection Officer and/or the Force Solicitor prior to implementation.

INFORMATION SECURITY.

UKGDPR, Article 5(f), and The Data Protection Act Part 3 Section 40, requires the Wiltshire Police and OPCC to ensure information is appropriately and adequately secured and that reasonable steps are taken to ensure the reliability of any employees who have access to personal data. Information Security refers to not only the physical or technical protective measures taken but also to issues such as the clear desk policy, use of e-mail and the Internet and the Government Security Classification (GSC). For further guidance, see the Information Security Policy.

In order to fulfil its statutory obligations, Wiltshire Police and the OPCC has implemented the provisions of the DPA 2018 in all respects, and follows the guidance contained in the College of Policing APP, the NPCC Data Protection Manual of Guidance and ICO guides.

POLICY AIM.

To ensure that all Wiltshire Police officers and staff, OPCC staff and 3rd parties are aware of their individual responsibilities in respect of the Data Protection legislation and to provide guidance to personnel in respect of the general requirements of the legislation.

APPLICABILITY.

Every police officer, member of police and OPCC staff and 3rd parties working for or on behalf of the police having access to personal data is required to comply with the requirements of the Data Protection legislation and any supporting local policy or procedure designed to help achieve compliance.

RELATED DOCUMENTS and Authorised Professional Practice.

APP > Information Management > Data Protection
Data Breach Notification Procedure
Information Sharing Policy
Information Risk Management Policy
Information Security Policy
Freedom of Information Policy (APP)
Niche RMS Minimum Data Quality Standards
Record Deletion, Amendment and Restriction Policy
Records Management Policy

Records Retention Schedule
NPCC Data Protection Manual of Guidance
ICO Data Protection Guidance

DATA PROTECTION AND FREEDOM OF INFORMATION.

The Force Data Protection Policy is compliant with the Data Protection legislation.

This document has been assessed as suitable for public release.

HUMAN RIGHTS AND EQUALITY IMPACT.

This policy has been drafted to comply with the principles of the Human Rights Act 1998 and Equality Act 2010. Members of Wiltshire Police administering this policy are responsible for ensuring that in its application, those to whom the policy applies, shall not receive less favourable treatment because of their age, colour, disability, ethnic or national origin, gender re-assignment, marital status, nationality, race, religion, sex or sexual orientation.

This policy has been subject to an equality impact assessment and has been graded Low Impact.

Revision History

Version	Date	Summary of Changes
4.0	17.08.2022	2 year review completed and updates to reflect UKGDPR.
4.0	24.08.2022	Reference and applicability to the OPCC added and made clearer.
5.0	15.04.2024	Review and update. Policy adapted onto new SharePoint template.