WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Data Protection**
POLICY REFERENCE NO:	**Inf/03**

Executive Summary.

The purpose of this Policy document and supporting procedures is to set out the commitment of West Midlands Police (WMP) to ensuring compliance with the Data Protection Act 2018 (DPA2018) which includes the General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED).

This Policy has been checked against APP. WMP has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by WMP. Those provisions are shown in the link below and can be accessed via the home page of the APP website:

https://www.app.college.police.uk/app-content/information-management/data-protection/

***Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.*

Intended Policy Audience.

This Policy applies to all WMP Force personnel, i.e. Police Officers, Police Staff, Police Community Support Officers, Special Constables, volunteers, partners, agency or temporary staff, subcontractors and third-party suppliers who may use WMP information systems. Only current employees and vetted personnel as listed above will be granted access to WMP equipment, data and information systems.

Current Version And Effective Date.	**2.0**	**01/02/2019**
Business Area Owner	**Information Management**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries, Assistant Director, Information Management**	
Policy Author	**Steven Yates, SIRA, Information Management**	
Approved By	**CC David Thompson**	
Policy Initial Implementation Date	**12/01/2016**	
Review Date	**21/07/2021**	
Protective Marking	**Official**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- *APP* https://www.app.college.police.uk/app-content/information-management/data-protection/
- *Code of Ethics (*http://www.college.police.uk/What-we-do/Ethics/Pages/Code-of-Ethics.aspx)

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Vision

Preventing crime, protecting the public and helping those in need.

Force Diversity Vision Statement and Values

“Maximise the potential of people from all backgrounds through a culture of fairness and inclusion to deliver the best service for our communities”

“All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay.

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position.
Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/What-we-do/Ethics/Pages/Code-of-Ethics.aspx for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organisation to do the right thing.

CONTENTS

Acronyms

- DPA2018 – Data Protection Act 2018
- GDPR – General Data Protection Regulation
- LED – Law Enforcement Directive
- DPO – Data Protection Officer
- SIRO – Senior Information Risk Officer
- ICO – Information Commissioner's Office

1. POLICY STATEMENTS.

1.1. WMP has a legal obligation to comply with the DPA2018, incorporating the GDPR and the LED. These combined documents and legislation establish the standards and governs the processing of personal data. WMP will ensure full compliance with all legal and regulatory requirements to fulfil this obligation.

1.2. WMP recognises that all data and information is a valuable asset, essential for effective police operations. Article 5 (2) of the DPA2018 (the Act) states that Data Controllers shall be responsible for, and able to demonstrate compliance with the data protection principles contained within the Act. The Chief Constable is the Data Controller for WMP and has appointed a Data Protection Officer (DPO) to direct the day-to-day operation of the DPA2018 within WMP.

1.3. WMP will implement a governance framework to support the Chief Constable and Senior Information Risk Owner (SIRO) in the effective management of data protection. The framework will be based on current HMG guidelines, all applicable legislation, and be reflective of commercial best practice. It will include the appropriate documentation of current and future data processing processes across all areas of police business and identification of the basis for processing both Personal Data and Special Category Personal Data.

1.4. This Policy is underpinned by procedural guidance (the Data Protection Procedure) that sets out minimum standards and details how those employees and any other authorised person having access to any Force systems may use Force-owned personal information lawfully and in accordance with regulations.

1.5. All Police Officers and Police Staff will receive training in Data Protection practices and are responsible for actively identifying data protection and security risks, contributing to appropriate data protection management strategies, and helping to embed an effective data protection culture within their teams.

1.6. WMP will take criminal and/or disciplinary action against any category of person mentioned above whom wilfully accesses and/or misuses personal information held by WMP. Any use of personal information that does not have a clear policing or other statutory or business purpose is likely to constitute a misuse. Section 170 of DPA2018 identifies the following criminal offences for the unlawful obtaining of personal data in that it is an offence for a person knowingly or recklessly:

- ✓ To obtain or disclose personal data without the consent of the Data Controller; OR
- ✓ To procure the disclosure of personal data to another person without the consent of the Data Controller; OR
- ✓ After obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal date when it was obtained.
- ✓ Section 171 and 172 of DPA2018 for re-identification of de-identified personal data, states it is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the Data Controller responsible for de-identifying the person data.

1.7. Where applicable and defined, all WMP staff will carry out the obligations of their individual role as defined in the Information Risk Management Policy.

1.8. WMP will publish and maintain a Data Protection Privacy Notice which describes the key aspects of personal data being processed. This includes: what personal data is collected and why, how it is collected, processed, shared, retained, disposed of, and kept secure. The Notice will also describe how data subjects can contact the WMP DPO to make enquiries or complaints about personal data being kept by WMP.

1.9. WMP will ensure that information security requirements for protecting personal data are met by working with the entire organisation to ensure the confidentiality, integrity, and availability of police information.

1.10. WMP will submit and maintain annual registration with the Information Commissioner's Office (ICO) in line with DPA2018 obligations.

1.11. WMP will conduct appropriate Data Protection Impact Assessments (DPIAs) for all new and current projects where personal data is being processed to establish any potential data protection issues and ensure mitigation is put in place at an early stage in each project's lifecycle.

1.12. The rights of individuals in relation to their personal data, as defined in the DPA2018, shall be respected at all times by WMP.

1.13. WMP will implement an audit and review framework (the Compliance, Audit and Assurance Procedure) to routinely test compliance against this Data Protection Policy, supporting procedures and processes to identify data protection risks, along with corrective and mitigating actions.

1.14. Compliance with this Policy will ensure:

- ✓ The protection of WMP's reputation;
- ✓ That all Officers and Staff will process personal information lawfully in accordance with the Act;
- ✓ The protection of individuals (data subjects) from the use of inaccurate personal information and the misuse of accurate personal information; and
- ✓ The safeguarding of personal data at every level of processing.

1.15. WMP qualify as a 'Competent Authority' under the LED (Section 30 of Chapter 1 to the Act) and will similarly demonstrate compliance with all relevant Directive requirements to protect individuals.

2. EQUALITY IMPACT ASSESSMENT (EQIA).

2.1. The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how WMP has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

3. HUMAN RIGHTS.

3.1. This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

4. FREEDOM OF INFORMATION (FOI).

4.1. All official policy/procedural guidance documents will be considered for publication under the principles of FOI on the external website for public disclosure. Please see the ICO Definition Document for Police Forces for further details https://ico.org.uk/media/for-organisations/documents/1280/definition_document_for_police_forces.pdf

5. TRAINING.

All Police Officers and Police Staff will receive training in Data Protection practices and are responsible for actively identifying data protection and security risks, contributing to appropriate data protection management strategies, and helping to embed an effective data protection culture within their teams.

6. PROMOTION / DISTRIBUTION & MARKETING.

6.1. The following methods will be adopted to ensure full knowledge of the Policy:

- Publication on force Policy Portal
- Noticeboard message

7. REVIEW.

7.1. The policy business owner Information Security maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

7.2. The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

7.3. A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted by the date shown as indicated on the first page.

7.4. Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

7.5. Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

CHIEF CONSTABLE

8. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
1.1	05/09/12	Policy Review (supersedes Part 1 order 14/2000)	51264 Firkins
1.2	18/09/12	Presentation amendments	4566 Brookes
1.3	03/01/2013	To Command Team for approval	Mr Chris Price
1.4	11.01.2013	To CC for authorisation	CC Chris Sims
1.5	12/01/2015	Review; section 9 updated to include Lawful of Handling Information training.	51264 Firkins
1.5	13/01/2015	Formatting adjusted before publication, Standard Code of Ethics section included	56408 Parkinson
2.0	11/04/2019	Policy reviewed and put onto new template style – transferred back onto old style for sign off	56408 Parkinson/58687 Yates
2.0	21/07/2019	Policy approved by CC	56408 Parkinson

9. PROCEDURAL GUIDANCE.

(See Policy Portal – Data Protection Policy page for copy)

DATA PROTECTION PROCEDURE

COMPLIANCE, AUDIT AND ASSURANCE PROCEDURE

WMP PRIVACY NOTICE WEBPAGE

INFORMATION RISK MANAGEMENT POLICY (See Information Risk Management Policy Page)