



# DATA SUBJECTS RIGHTS POLICY

## Executive Summary

This policy sets out how West Midlands Police (WMP) upholds the data subject rights of individuals in accordance with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) (including Part 3 – Law Enforcement Processing), the Human Rights Act 1998, Data Use and Access Bill and other relevant legislation. It ensures that individuals' rights are respected while enabling the Force to carry out its policing duties effectively, lawfully, and proportionately.

## Authorised Professional Practice (APP)

WMP have adopted the [APP](#), with supplementary information contained herein, which reflects local practice and the needs of the communities served by WMP.

## Scope

The Chief Constable has overall direction and control of WMP and is accountable for all policies and supporting documents of the organisation and its actions. Adherence to this force policy will be expected from all employees and representatives of WMP. It applies to all personal data processed by the Force, all officers, staff, volunteers, contractors, and partner agencies acting on behalf of the Force. The personal information covered by this policy is stored in all systems, applications, databases, and hardcopy records used for policing or corporate purposes.

## Objectives

This policy aims to:

- Demonstrate how WMP complies with data subjects' rights in line with The Data Protection Act 2018 and GDPR.

## Definitions/Acronyms

|                     |                                                                                                                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Subject</b> | The data subject is the person who is exercising their rights.<br>Anyone can exercise their rights; be it a victim, suspect, witness or employee.                                                                                                                                                                            |
| <b>DPA 2018</b>     | The UK's primary data protection law. It sets strict rules for how organizations and the government collect, store, and process personal information. Operating alongside the UK General Data Protection Regulation (UK GDPR), its primary goal is to protect privacy and give individuals control over their personal data. |
| <b>UK GDPR</b>      | Sets strict rules on how organizations, businesses, and the government can collect, store, and process your personal information.                                                                                                                                                                                            |
| <b>WMP</b>          | West Midlands Police                                                                                                                                                                                                                                                                                                         |

## Policy Statements

### 1. DATA PROTECTION RIGHTS

- 1.1 Under UK GDPR and the DPA 2018, individuals have the following rights. Some rights may be restricted where necessary and proportionate for policing purposes, as permitted by law.

### 2. RIGHT TO BE INFORMED



- 2.1 Individuals have the right to clear information about how their data is collected, used, shared, and retained.
- 2.2 The Force meets this through:
  - Privacy notices
  - Public facing transparency information
  - Operational notices where appropriate
- 2.3 Restrictions may apply where providing information would prejudice policing purposes.

### **3. RIGHT OF ACCESS (SUBJECT ACCESS REQUEST – SAR)**

- 3.1 Individuals have the right to access and receive a copy of their personal data and other supplementary information. This is commonly referred to as a subject access request or SAR
- 3.2 Individuals can make SARs verbally or in writing, including via social media. A third party can also make a SAR on behalf of another person, with the appropriate authority to act on their behalf.
- 3.3 Information must relate to the individual to be personal data. This means that it does more than simply identifying them it must concern the individual in some way. Data can reference an individual and not be personal data. For example, just because someone's name is on an incident log, it does not mean the data belongs to them.
- 3.4 In most circumstances we will not charge a fee to deal with a request.
- 3.5 We should respond within one calendar month of receipt of the request, unless a permitted extension is relied upon. If we are going to need extra time to deal with a request, we will communicate that to the data subject within one calendar month.
- 3.6 We can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

### **4. IDENTIFYING VALID AND NON-VALID REQUESTS.**

- 4.1 Requests for information should be sent to the data protection inbox. These can be by email or via our external website using the digital form. Any applications submitted by post will be processed by the Business Support Assistants who will scan them in and email them to the inbox
- 4.2 For a request to be valid we require the applicants full name and date of birth, a description of the information that they are looking for and 2 forms of ID, which between them show the applicants name, current postal address, date of birth and signature
- 4.3 We have a WA162 application form which applicants can complete; however, this is not mandatory. In the absence of a signed application form we will ask applicants to send us a copy of their signature to cross reference with their ID.
- 4.4 While a form, or email, is the most efficient way to obtain a request, we cannot insist an individual submits their request in a specific way. Therefore, if someone makes a request verbally and does



not want to complete a form/send an email, it is your responsibility to ensure that the request is passed onto the Data Protection team in order for them to contact the data subject.

## **5. REQUESTS SUBMITTED WITH THIRD PARTY AUTHORISATION**

- 5.1 Data subjects can appoint third parties to act on their behalf. This can be their solicitor, charities or they can ask someone they know to represent them.
- 5.2 Before the request is accepted, we require a signed letter of authority from the data subject, which authorises the release of their information to another party.
- 5.3 If the data subject does not have capacity, we require proof that the representative has Power of Attorney.
- 5.4 If the applicant has parental responsibility or legal guardianship, we require a copy of the birth certificate or legal papers confirming this.

## **6. PARENTAL RESPONSIBILITY**

- 6.1 In some cases, it is possible for information about children to be released to a person with parental responsibility. However, the best interests of the child will always be considered. Even if a child is very young, data about them is still their personal data and does not belong to anyone else. It is the child who has a right of access to the information held about them
- 6.2 12 years old is the age that children are presumed to be mature enough to have a general understanding of their data protection rights, however each request will be assessed to understand the child's level of understanding

## **7. COMPLEX SARS**

- 7.1 There are instances where providing the data subject the requested information within the time period stated is not possible, this could be due to the nature of the information, volume of data requested, sensitivity or operational context. In these instances the Force is permitted to extend the time from by up to two additional months, but must ensure they provide the requestor with prompt clear justification around the extension within one calendar month.

## **8. VEXATIOUS OR MANIFESTLY UNFOUNDED REQUESTS**

- 8.1 The Force will assess requests to determine whether they are manifestly unfounded or excessive based on evidence, behaviour and context rather than the requestor's identity or motives. The Force may refuse a request where it is clear that the request or requestor is clearly malicious, abusive, repetitive, disproportionate or submitted with no genuine intention to access the personal data.
- 8.2 Where the request is deemed excessive the Force are permitted to charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.



- 8.3 In both instances the Force will provide the requestor with a refusal notice, setting out the reason for the refusal and providing the requestor with details on how to complain to the Information Commissioner's Officer if they so wish.

## **9. RIGHT TO RECTIFICATION AND RIGHT TO ERASURE**

- 9.1 Individuals have the right to request any inaccurate / incomplete data is amended or deleted. As a Competent Authority, West Midlands Police retain accurate records of allegations made at the time or reporting and throughout the investigative process, even if the allegations are unfounded or No Further Actioned (NFA). These records are retained under our statutory functions and where processing is necessary for the performance of a task carried out by a competent authority.
- 9.2 The definition of statutory function for 'law enforcement purposes' is 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.
- 9.3 Law enforcement data is retained under our Retention Schedule which relies on the Management of Police Information Groups (MoPI) and clear periods of time with no offending or other relevant information being recorded against their name.
- 9.4 Requests for rectification or erasure can be accepted verbally or in writing. Due to the sensitive nature of the information we process, West Midlands Police will always require photographic identification to validate a data subject's identity. If a request is received it will follow the same process as receiving a Subject Access Request.
- 9.5 In some instances where erasure is not possible, the Force may restrict processing instead.

## **10. RIGHT TO RESTRICT PROCESSING**

- 10.1 Under certain circumstances individuals have the right to ask us to restrict the processing of their personal data. This may be in cases where:
- They are contesting the accuracy of their personal data while we are verifying the accuracy
  - The information has been unlawfully processed and they oppose its erasure and have requested a restriction instead
  - where we no longer require the personal data but you need it to establish, exercise or defend a legal claim and do not want us to delete it.

## **11. RIGHT TO DATA PORTABILITY**

- 11.1 Individuals have the right to obtain and reuse their personal information for their own purposes, transferring it from one environment to another. This right only applies to personal data provided by an individual, where the processing is based on their consent or for the performance of a contract and when that processing is carried out by automated means. This right is not applicable to data we process under Part 3 Law Enforcement Processing.



## **12. RIGHT TO OBJECT**

- 12.1 Individuals have the right to object to processing of personal data if:
- processing based on legitimate interests or performance of a task in the public interest and or exercise of official authority
  - processing of their information for scientific and historical research and statistics
  - direct marketing
- 12.2 Any objection must be on grounds relating to individual situations.
- 12.3 This right is not applicable to data we process under Part 3 Law Enforcement Processing.

## **13. RIGHTS RELATED TO AUTOMATED DECISION MAKING AND PROFILING**

- 13.1 Individuals have the right not to be subject to a decision when it is based on solely automated processing (including profiling) and which produces a legal effect or similar significant effect on them.
- 13.2 This right does not apply if the decision is:
- authorised by law
  - is necessary for entering into or performance of a contract
  - is based on your consent
- 13.3 We are unlikely to carry out automated decision making as our processes involve some type of human interaction and decision-making.
- 13.4 Profiling is any form of automated processing of personal data intended to evaluate certain personal aspects about individuals to predict things about them such as their behaviours, interests, movements or performance at work. We do not currently carry out automated profiling.

## **14. EXERCISING RIGHTS**

- 14.1 Any requests received from individuals wishing to exercise any of the above rights should be directed to the Data Protection Inbox.

## **15. ROLES AND RESPONSIBILITIES**

- 15.1 **Data Protection Officer (DPO)**
- Responsible for compliance with data protection across the organisation and liaising with the supervisory authority (ICO)
- 15.2 **Data Protection Team**
- The data protection team will process requests for data subjects to exercise their rights. The team provide an administrative function for all GDPR rights, but will also process subject access requests.
- 15.3 **Records Management Team**



- The records management team work alongside the data protection team, and process requests in relation to deletion and rectification.

## **Relevant Legislation / Policies / Procedural Guidance**

The Force recognises and complies with the rights provided under:

- UK GDPR (for non-law enforcement processing)
- Data Protection Act 2018 Part 3 (for law enforcement processing)
- Data Use and Access Act
- Human Rights Act 1998 – Article 8 right to privacy
- [ICO Right of Access guidance](#)
- [ICO Guide to Subject Access](#)

## **Equality Impact Assessment**



WMP places trust in their employees to comply with force policies and to work in accordance with and in support of:

- [WMP Vision and Values](#)
- [Code of Ethics | College of Policing](#)
- [Voice of the Child](#)

|                                                      | What impact has this policy <b>had</b> on the nine protected characteristics in relation to the three general duties? (If applicable) | How <b>will</b> this updated policy positively impact each of the nine protected characteristics in relation to the three general duties? If not, explain why it will not.                                                       |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Age</b><br>(including children and young persons) | There are no adverse impacts on this protected characteristic                                                                         | This policy will positively impact on children's data specifically as it sets out the fact the organisation recognises parental responsibility does not automatically entitle a parent to a copy of their child's personal data. |
| <b>Disability</b>                                    | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Gender Reassignment</b>                           | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Pregnancy &amp; Maternity</b>                     | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Marriage &amp; Civil Partnership</b>              | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Race</b>                                          | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Religion or Belief</b>                            | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Sex</b>                                           | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |
| <b>Sexual Orientation</b>                            | There are no adverse impacts on this protected characteristic                                                                         | No anticipated positive impact.                                                                                                                                                                                                  |

## Publication Instructions

Suitable for publication to public

## Document Control

|                                             |                                                                            |
|---------------------------------------------|----------------------------------------------------------------------------|
| <b>Strategic Lead:</b><br>[role and name]   | ██████████<br>████████████████████████████████████████                     |
| <b>Policy Author(s):</b><br>[role and name] | ██████████<br>████████████████████████████████████████████████████████████ |
| <b>Effective Date:</b>                      | 30.06.2026                                                                 |



|                                            |                                                 |
|--------------------------------------------|-------------------------------------------------|
| <b>FET Lead:</b><br><i>[role and name]</i> | Peter Gillet<br>Director of Commercial Services |
| <b>Version Number:</b>                     | V1.0                                            |
| <b>Review Date:</b>                        | 30.06.2028                                      |

Any enquiries in relation to this policy should be made directly with the Strategic Lead.

All policies are subject to a formal consultation process which encompasses Legal, Professional Standards, Faith Groups, Trade Unions, Independent Advisory Groups and wider force groups and any other relevant parties. A record of consultation can be found on the Policy Portal.

It is responsibility of the Strategic Lead to ensure that all links within the policy are correct and accessible.

**Amendment History:**

| Version Number: | Effective Date: | Summary of Amendments: | Author: |
|-----------------|-----------------|------------------------|---------|
|                 |                 |                        |         |