**Date:** 12/02/2025
**Our ref:** 01/FOI/25/014115/U

**FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/25/014115/U**

I write in connection with your request for information dated 03/02/2025, received by Greater Manchester Police (GMP) for the following information:

***A copy of your organisation's data protection policy for the relevant period***

***Clarification – Most up to date version please.***

**Result of Searches**
Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm the information requested is held by GMP.

I am not obliged to supply you with all the information as an exemption applies.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because this information is exempt) to provide you, the applicant, with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies. The information you have requested is exempt from disclosure by virtue of the following exemption: Section 40(2) – Personal Information.

Where redactions occur, this represents information that identifies a living individual, to disclose this information would breach the principles of the GDPR and the Data Protection Act 2018. Personal data is defined by Article 4 of the GDPR and Part 1 of the Data Protection Act 2018 and means any information relating to an identified or identifiable natural person ('data subject'). An identified natural person is one who can be identified directly or indirectly from that data.

**Please see the attached document.**

# Data Protection

# Policy

## Greater Manchester Police

## January 2023

**POLICY IMPLEMENTED:** January 2023

**REVIEW DATE:** January 2025

**POLICY OWNER:** [redacted]

**APPROVED BY:** [redacted]

**IS THE POLICY NEW OR REVISED?** Revised

| VERSION NO | DATE | SUMMARY OF CHANGES | AUTHOR(S) | PUBLISHED ON CCOs |
|---|---|---|---|---|
| 1.0 | Jun 2003 | [redacted] | [redacted] | [redacted] |
| 1.1 | 17/08/2011 | Draft Review of policy. | [redacted] | |
| 1.2 | 19/10/2011 | Minor amendments/additions. | [redacted] | |
| 1.3 | 06/12/2011 | Transfer to corporate template and minor amendments. | [redacted] | |
| 1.4 | 16/01/2012 | Minor amendments. | [redacted] | |
| 1.5 | 22/02/2012 | Amendments approval by [redacted]. | [redacted] | |
| 2.0 | April 2012 | Minor [redacted] approval. | [redacted] | [redacted] |
| 2.1 | Oct 2014 | Transfer to new Policy & Procedure template and updated references. | [redacted] | |
| 2.2 | Oct 2016 | Section on training revised to reflect changes in Ncalt and the requirement to refresh training every three years. | [redacted] | |
| 3.0 | Jan 2023 | Changed from policy & procedure to a policy with associated procedures, along with full content review. | [redacted] | |
| | | | | |
| | | | | |

## Table of Contents

# 1. Policy Statement

GMP needs to collect and use certain types of information about the individuals or service users who come into contact with the force. This personal information must be collected and dealt with appropriately, whether is collected on paper, stored in a computer database or recorded on other material.

GMP is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). GMP needs to process certain personal data as defined by the DPA 2018 in order to fulfil its purpose and to meet its legal obligations. GMP will process such information according to the 6 Data Protection Principles:

1. Data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
2. Data shall be obtained for only one or more of the purposes specified within the DPA 2018, and shall not be processed in any manner incompatible with that purpose or those purposes;
3. Data shall be adequate, relevant and not excessive in relation to those purpose(s);
4. Data shall be accurate and, where necessary, kept up to date;
5. Data shall not be kept for longer than is necessary;
6. Data shall be kept secure by the Data Controller who takes the appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information.

## 1.1 Part 3 Processing (Law Enforcement)

Part 3 of the DPA applies to competent authorities that process personal data for ‘law enforcement purposes’ and covers processing “for 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”.

The principles are broadly the same as those in the UK GDPR, and are compatible so will assist in managing processing across the two regimes. Transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation and we must be able to demonstrate overall compliance with all of the Law Enforcement Principles which are:

1. Processing of personal data for any of the law enforcement purposes must be lawful and fair;

2. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and; Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected;

3. Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed;

4. Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and; Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay;

5. Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need of the continued storage of personal data for any of the law enforcement purposes;

6. Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

## 1.2 Data Sharing & Disclosure

GMP may share data with other agencies such as Greater Manchester Combined Authority (GMCA), other local authorities, victim services, funding bodies and other voluntary agencies. This is not an exhaustive list and more information regarding data sharing is contained within GMP's Register of Processing Activities (RoPA).

Individuals will be made aware, via Privacy Notices, of how and with whom their information will be shared in all circumstances unless a documented and justified exemption is applied. There are circumstances where the law allows GMP to process data (including sensitive data) without the data subject's consent. These can include:

- When carrying out a legal duty or as authorised by the Secretary of State
- When protecting the vital interest of an individual or other person
- Where the individual has already made the information public
- When conducting legal proceedings, obtaining legal advice or defending any legal rights
- For the monitoring of equal opportunities – i.e. race, disability or religion
- When providing a service where the individual's consent cannot be obtained or where it is reasonable to proceed without consent, e.g. to avoid causing stress

GMP will, through appropriate management and strict application of criteria and controls:

- Observe the conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Ensure the rights of people about whom information is held, can be fully exercised under the DPA 2018. These include:

  - The right to be informed that processing is being undertaken
  - The right of access to one's personal information
  - The right to prevent processing in certain circumstances
  - The right to correct, rectify, block or erase information which is regarded as incorrect information
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Treat people justly and fairly whatever their age, religions, disability, gender, sexual orientation or ethnicity when dealing with requests for information;
- Set out clear procedures for responding to requests for information.

## 1.3 Data Collection

It is GMP's policy to strictly follow the Data Protection Principles when collecting individuals' personal data. To ensure the protection of the rights and freedoms of the data subjects whose information GMP collects and processes, you must:

- Exercise care when collecting, processing or disclosing any personal data on behalf of GMP and do so only when it is necessary for your duties and it supports a lawful purpose.

- If relying on consent as the lawful basis for processing personal data involving children, GMP must verify in these circumstances that the data subject is old enough to provide consent. In the UK, only children aged 13 or over are able provide their own consent.

- Ensure the information you record is accurate, adequate for the purpose, not excessive, and worded clearly and unambiguously, e.g. all fields are completed with relevant, meaningful and correct information; check existing records to make sure you are not creating duplicates and do not take short cuts / skip fields that should be completed.

- Do not record irrelevant or inappropriate remarks about individuals because anyone has a right to see personal information that we hold; this could lead to claims for compensation and/or enforcement action against the force. Be aware that any data, that you create and record, whether personal or not, is potentially disclosable under the DPA 2018, UK GDPR, FOI or EIR.

- Abide by force retention guidelines (see GMP Retention and Disposal Procedures), do not keep information longer than is necessary and do not keep copies of information "just in case" beyond their retention periods.

- Ensure appropriate security of the information against unauthorised or unlawful processing and against accident loss, destruction or damage at all times. This is especially important if the information is required to be carried out of police premises

– it should not be left unattended at any time. If the information is held on portable media it should be encrypted in case of loss.

## 1.4 Data Storage

Information and records relating to individuals will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is GMP's responsibility to ensure that all personal and organisational data is non-recoverable from any computer system previously used within GMP which has been passed on or sold to a third party.

## 1.5 Data Access and Accuracy

All individuals have the right to access the information that GMP holds about them. GMP will also take reasonable steps to ensure that this information is kept up to date by liaising with data subjects regarding any changes. In addition, GMP will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection;
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- Everyone processing personal information is appropriately trained to do so;
- Everyone processing personal information is appropriately supervised;
- Any member of staff wanting to make enquiries about handling personal information knows what to do;
- It deals promptly and courteously with any enquires about handling personal information;
- It clearly describes how it handles personal information;
- It will regularly review and audit the way it holds, manages and uses personal information.

## 1.6 Training

As part of GMP's ongoing commitment to implementing and further developing this policy, it is committed to regularly educating and training employees to raise their awareness of the policy and of any further commitments required by GMP to conform with legislation.

Compliance with data protection legislation, and other mandatory legislative and regulatory requirements, is an identified training objective for GMP employees. Training shall be delivered to all staff on a periodic basis to ensure an appropriate level of knowledge and awareness, as dictated by their roles and responsibilities within the organisation and taking into account the quantity and sensitivity of the information they will have access to.

## 1.7 Monitoring

This policy will be continually monitored and subject to regular review. It will be updated as necessary to reflect best practice in data management, security and control to ensure compliance with any changes or amendments made to the Data Protection Act.

## 1.8 Non-Conformance

There is a requirement for all employees to comply with this policy, and where requested, to demonstrate such compliance. Failure to comply with the policy shall be regarded as a disciplinary offence and shall be dealt with as defined in the Disciplinary Policy.

In addition to disciplinary action, the Data Protection Act 2018 makes it an offence to knowingly or recklessly obtain, retain, use, distribute, disclose or destroy personal information without authorisation. In these circumstances such behaviour can be considered to be a criminal offence and result in prosecution.

Unauthorised use or loss of the data is a breach of these regulations and the Force could be issued with a monetary penalty of up to £17.5 million. Deliberately accessing/processing information without authority could be a criminal offence for which the individual would be personally liable.

## 1.9 Specific roles and responsibilities

The **Chief Constable** of GMP is the notified **Data Controller** for the purposes of the DPA 2018 and UK GDPR. As such, they are obliged to ensure that GMP handles all personal data in accordance with Data Protection legislation.

**Senior Information Risk Owner** - takes responsibility for managing risk associated with information compliance matters.

**Force Data Protection Officer -** the lead on data protection policy and procedure; assists with monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for the supervisory authority, the Information Commissioner (ICO).

**Information Asset Owner (IAO) -** the owner of an Information Asset is responsible for ensuring that the asset is managed appropriately, in compliance with the legislation, to meet the requirements of the organisation, and any risks and opportunities are monitored.

**Information Asset Administrator (IAA)** - nominated by the IAO and is responsible for the day to day management of the information asset and its entry in the Information Asset Register.

**Information Compliance and Records Management Unit** (ICRMU) - data protection subject matter experts for the Force. A list of contacts is available on the intranet. The Unit is responsible for:

- Handling requests for information under: UK GDPR and DPA 2018 (Art. 15 UK GDPR and S.45 DPA – subject access); Freedom of Information Act (FOI), Environmental Information Regulations (EIR); from insurance companies under the ACPO/ABI agreement and the Criminal Injuries Compensation Authority (CICA).
- Advising on statutory compliance for all business processes and personal data disclosures to other organisations; Review any requests for data held by GMP to be deleted or corrected by data subjects, handling data protection complaints from the ICO and data subjects, review Data Protection Impact Assessments, developing information sharing and data processing agreements/contracts with third party processors, undertaking audits of force systems, and promoting good practice.

**Third Party Data Processors -** Where external companies are used to process personal data on behalf of GMP, much of the responsibility for the security and appropriate use of that data remains with the force. A Processor must be able to provide sufficient guarantees to implement appropriate technical and organisational measures to protect the processing of personal data in accordance with the legislation and support GMP with its data protection compliance requirements. They must only act on the documented instructions of GMP, but they still have direct responsibilities under the legislation, and may be subject to sanctions from the regulator (ICO) if they do not comply.

**Information Security -** the Information Security and Risk Lead and manager assure the security of IT systems.

**Professional Standards Branch -** investigate potential misconduct in relation to breaches of data protection and information security.

**All officers/staff:** Should be aware of their responsibilities under the legislation and in relation to the handling and processing of personal data. Compliance with DPA 2018 and UK GDPR is the responsibility of all employees who process personal data.

## 2. Scope

This policy applies to all GMP employees or third-party organisations that process personal data held by GMP as defined by the DPA 2018.

## 3. Terms and Definitions

**Competent Authority** - A person specified or described in Schedule 7 of the DPA 2018; and any other person if, and to the extent that, the person has statutory functions for the law enforcement purposes.

**Data controller** - A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.

**Data subject** - The identified or identifiable living individual to whom personal data relates.

**Data processor** - A person, public authority, agency or other body which processes personal data on behalf of the controller.

**Data Protection Impact Assessment** - A DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in high risk to the rights and freedoms of individuals. The Force must, prior to processing, carry out a DPIA which should include a general description of the processing operations, assessment of the risks to the rights and freedoms of those data subjects and measures to mitigate those risks. Those measures will demonstrate compliance and take into account the rights and legitimate interests of the data subjects and other people concerned.

**Information Asset** - A body of information, defined and managed as a single unit/record so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

**Information Asset Register** - A mechanism for understanding and managing an organisation's assets and the risks to them; including the links between the information assets, their business requirements and technical dependencies.

**Personal data** - Any information relating to an identified or identifiable natural person; 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.

**Personal data breach** - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

**Processing** - In relation to personal data, this means any operation or set of operations which is performed on personal data or on sets of personal data.

**Special Category Data** - These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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.

## 4. Associated Documents

- Data Protection Act 2018
- Computer Misuse Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003
- Register of Processing Activities (RoPA)
- Disciplinary Policy
- Personal Data Breach Policy (DRAFT)
- Information Sharing Policy (DRAFT)
- Privacy Notice
- Data Protection Impact Assessment Procedure

# 5. Statutory Compliance & Consultation

## 5.1 Statutory Compliance

### 5.1.1 Equality Act (2010)

This policy applies equally to the protected characteristics. It relates to compliance with the Data Protection Act and the provision of individual rights afforded by that Act and by the Human Rights Act.

Sensitive personal data as defined by the Act includes race, religion or belief, sexual life and additional obligations are placed on the data controller by the Act when processing data of this nature.

### 5.1.2 The General Data Protection Regulation (UK GDPR) and Data Protection Act (2018)

This policy has been produced by the Information Compliance & Records Management Unit and complies with the Data Protection Act 2018.

### 5.1.3 Freedom of Information Act (2000)

The Freedom of Information Act 2000 (FOIA) grants a general right of access to all types of recorded information held by public authorities, which may include stop and search data. This policy has been assessed as disclosable upon request under Freedom of Information. It is intended to be a public document and available upon request to members of the public and interested parties.

However, any requests for its disclosure should be directed through the Information Compliance and Records Management Unit via the Freedom of Information mailbox. [redacted].

## 5.2 Consultation

| Consulted | Comments |
|---|---|
| IS Branch | Due to the specialised nature of this policy, it has been developed purely by staff within ICRMU. |
| Police Federation – Tim Hanson | Numerous comments made, policy amended in section 1.8 to include additional reference to non-conformance. |
| Trade unions - UNISON, GMB | None |
| Legal Services | None |
| Force Crime & Incident Registrar | None |
| Staff Associations | None |
| Staff Support Networks | None |
| HR | Queried whether it included data held about our own staff, but it doesn't as these are outlined in privacy notices. No amendments required. |