



**METROPOLITAN
POLICE**

TOTAL POLICING

Freedom of Information Act Publication Scheme	
Protective Marking	Not Protectively Marked
Publication Scheme Y/N	Yes
Title	MPS Privacy Notice
Version	
Summary	To explain how the MPS processes personal/ sensitive personal data relating to members of the public.
(B)OCU or Unit, Directorate	Met HQ Strategy & Governance - Information Right's Unit
Author	
Review Date	September 2023
Date Issued	October 2019

MPS Privacy Notice

This privacy notice explains how and why the Metropolitan Police Service (MPS) processes your personal data, under PART 2 (General Data) and PART 3 (Law Enforcement Processing) and outlines the steps we take to ensure that personal data is protected and describes the rights individuals have in regards to their personal information and how to complain to the Information Commissioner if you have concerns as to how we have handled your data.

1. Data Controller

The Commissioner of the Metropolitan Police Service (MPS) is the controller for any personal data processed by the Met.

2. Data Protection Officer

The Data Protection Officer is Darren Curtis and can be contacted by email at: DataProtection_FreedomofInformationOfficer@met.police.uk

The Met's Information Rights Unit manages the Met's data protection compliance and can be contacted at: DPAMailbox-.ROAR@met.police.uk

3. What type of personal data do we process?

The MPS process personal data, including Special Categories of personal data that can be used to identify a living individual, on its own or in combination with other available information. References to names, identification numbers and location data would all be personal data. Processing means anything we do with the data and includes collecting, storing, and sharing that enables us to achieve our various roles this will include:

- Your name and address
- Family, lifestyle and social circumstances
- Education and training details
- Employment details
- Financial details
- Goods or services provided
- Offences and alleged offences
- Criminal proceedings, outcomes and sentences
- Sound and visual images including Body Worn Video and Facial Recognition

- References to manual records or files
- Information relating to safety and health
- Complaint, incident, civil litigation and accident details

The Special Categories that we hold include:

- Race
- Ethnic origin
- Politics
- Religion and beliefs
- Trade union membership
- Genetics
- Biometrics (such as DNA, fingerprints, facial images, and voice recordings)
- Mental and physical health
- Sex life, or sexual orientation
- Employment details

When we process special category data the following conditions will apply:

The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

Processing relates to personal data which are manifestly made public by the data subject.

Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Processing is necessary for reasons of substantial public interest, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to contract with a health.

Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

We may monitor and/or record and retain telephone calls, texts, emails, and other electronic communications in order to deter, prevent, and detect inappropriate or criminal activity, to ensure we are accountable for our behaviour, and to ensure security. Your personal information may be held on a computer system, in a paper record such as in a physical file or a photograph.

Processing is necessary in order to carry out Staff Survey this will include allowing third parties working on the MPS behalf access to Staff data so they can carry out work on the staff survey.

4. Whose data do we hold?

We may obtain, use, and disclose personal information relating to a wide variety of individuals including, but not limited to, the following:

- Existing and former MPS Police staff and police officers including volunteers, contractors, agents, and temporary / casual workers
- Former and potential members of staff, staff pensioners, and beneficiaries
- Suppliers
- Victims of crime and members of the public who report or witness police incidents
- Offenders and suspected offenders
- Missing persons, vulnerable persons, and children who are considered at risk
- Complainants, correspondents, and enquirers
- Relatives, guardians, and associates of subjects of interest whose personal data has been processed
- Advisers, consultants, interpreters, and other professional experts
- Other individuals necessarily identified in the course of police enquiries and activity

5. What is our lawful basis for processing personal data?

Each business process involving personal data is independently assessed to determine its lawful basis.

The overwhelming majority of personal data handled by Metropolitan Police is Law Enforcement Processing, and therefore is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

Law Enforcement Processing (PART 3) is defined by the Data Protection Act 2018 as information processed for the purpose of:

- Prevention, investigation, detection, or prosecution of criminal offences
- Execution of criminal penalties
- Safeguarding against, and preventing threats to, public security

Other business areas will process personal data because:

- It is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract
- The processing is necessary for us to comply with the law (not including contractual obligations)
- The processing is necessary to protect someone's life
- The individual has given clear consent for us to process their personal data for a specific purpose

Where we rely on your consent to process your personal data, we will make sure that it is a clear and unambiguous indication of your wishes, that your decision to give consent is fully informed, and that it is freely given. We will also give you certain information at the time of obtaining your consent, including:

- Any third party controllers who will rely on the consent
- Specify exactly what data we are collecting, what we want to do with it, and why we need it
- How to withdraw your consent if you change your mind at a later date

6. What do we do with personal data?

We obtain, hold, use, and disclose personal information for policing purposes including:

- Protecting life and property
- Preserving order

- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility of the police arising from common or statute law

We also obtain, hold, use, and disclose personal information to support policing purposes including:

- To be accountable to the public, to be regulated by external bodies, and to be audited by third parties
- Staff administration, including but not limited to, payroll and benefits, pensions, training and development, performance management, occupational health, and welfare of police officers and police staff including volunteers, agents, and temporary / casual workers
- Vetting of police officers and police staff, including volunteers, agents, and temporary / casual workers, and vetting of relevant third parties, including partners and suppliers
- Management of public relations, journalism, advertising and media
- Business Management including, but not limited to, finance and accounting, procurement, property, planning, insurance, vehicle fleet and transport (including driver behaviours), internal review, auditing, health and safety, information technology systems including systems testing, and legal services
- Management of correspondence, including complaints, requests for information, and other contacts from the public or other organisations
- Licensing, permit holding, and registration
- Research, including surveys
- Sports and recreation
- Security

We will only use appropriate personal information necessary to fulfil a particular purpose or purposes.

Personal information could be held on a computer or in a paper record. It can also include other types of electronically held information such as CCTV.

Sometimes we disclose personal data outside of the European Union. They may not have laws that protect the individual's right to privacy in a similar way to the United Kingdom (UK), but where this is the case, Metropolitan Police takes its own appropriate steps to ensure that personal data is protected in an equivalent way.

7. Where do we get data?

We may obtain personal information from a wide variety of sources including, but not limited to, the following:

- Police staff and police officers including volunteers, agents, and temporary / casual workers
- The Mayor's Office for Policing and Crime (MOPAC)
- Other law enforcement agencies, including international agencies and bodies
- Other parts of the criminal justice system including, but not limited to, legal representatives such as prosecuting or defending solicitors and barristers, prosecuting authorities like the Crown Prosecution Service, courts, and Prisons and Young Offenders Institutions
- Non-police agencies with prosecuting rights e.g. Trading Standards
- Providers of victim support services
- Central and local government, governmental agencies and departments, including Her Majesty's Revenue and Customs, other emergency services, and the NHS
- Healthcare, social care, and welfare advisers or practitioners
- Education, training establishments, and examining bodies
- Other government agencies, private sector organisations, and charities involved in crime and disorder and safeguarding strategies
- Licensing authorities
- Persons making an enquiry or complaint
- Regulatory bodies such as Independent Office for Police Conduct, Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, Ombudsmen, and other regulatory authorities
- Auditors
- Individuals themselves
- Relatives, guardians, or other persons associated with the individual including current, past, or prospective employers of the individual
- Trade Unions, employer associations, and professional bodies including, but not limited to, the Police Federation, Unison, and Unite
- Business associates and other professional advisors
- Suppliers, and other providers of goods or services

- Financial organisations and advisors, including credit reference agencies
- Survey and research organisations, including universities
- Security companies
- Approved organisations and people working with the police
- Data Processors working on behalf of MPS
- Voluntary and charitable organisations
- The media

We may also obtain personal information from other sources such as our own CCTV systems, body worn video cameras, live facial recognition technology including drones as well as local authority and privately owned CCTV systems, and documents and correspondence.

8. With whom do we share data?

We may disclose personal information to a wide variety of recipients in any part of the world, including those from whom personal information is obtained. This includes, but is not limited to:

- Police staff and police officers including volunteers, agents, and temporary / casual workers
- The Majors Office for Police and Crime (MOPAC)
- Other law enforcement agencies, including international agencies and bodies
- Other parts of the criminal justice system including, but not limited to, legal representatives such as prosecuting or defending solicitors and barristers, prosecuting authorities like the Crown Prosecution Service, courts, and Prisons and Young Offenders Institutions
- Non-police agencies with prosecuting rights e.g. Trading Standards
- Providers of victim support services
- Central and local government, governmental agencies and departments, including Her Majesty's Revenue and Customs, other emergency services, and the NHS
- Healthcare, social care, and welfare advisers or practitioners
- Education, training establishments, and examining bodies
- Other government agencies, private sector organisations, and charities involved in crime and disorder and safeguarding strategies
- Licensing authorities

- Persons making an enquiry or complaint
- Regulatory bodies such as Independent Office for Police Conduct, Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, Ombudsmen, and other regulatory authorities
- Auditors
- Individuals themselves
- Relatives, guardians, or other persons associated with the individual including current, past, or prospective employers of the individual
- Trade Unions, employer associations, and professional bodies including, but not limited to, the Police Federation, Unison, and Unite

Business associates and other professional advisors

- Suppliers, and other providers of goods or services
- Financial organisations and advisors, including credit reference agencies
- Survey and research organisations, including universities
- Security companies
- Approved organisations and people working with the police
- Data Processors working on behalf of MPS
- Voluntary and charitable organisations
- The media

We may also disclose information to prevent harm to individuals.

Disclosure of personal information will be made on a case-by-case basis with the necessary controls in place.

We will also disclose personal information to other bodies or individuals when required to do so by an act of legislation, rule of law, or by court order. This may include disclosures to the Child Support Agency, Children and Family Court Services, the National Fraud Initiative, the Home Office, Regulatory Bodies, and to the Courts.

We may also disclose personal information on a discretionary basis for the purpose of any legal proceedings or for obtaining legal advice.

9. Retention

We keep personal data as long as is necessary for the particular purpose(s) for which it is held.

Personal data which is placed on national police systems namely, the Police National Computer, National DNA Database or National Fingerprint Database is managed in accordance with [NPCC Deletion of Records from National Police Systems](#).

Other records containing personal data relating to crime recording, domestic violence, violent and sexual offenders, child abuse investigation, public protection, missing persons, case and custody, incident records, firearms licensing and intelligence will be retained in accordance with the [Authorised Professional Practice on the Management of Police Information](#).

Corporate and non-crime information (such as HR and financial records) will be retained in accordance with the MPS retention schedule.

10. Consent

Occasionally, where there are no other appropriate grounds, the Met may ask for your explicit consent in order to lawfully process your data. This will only happen in specific and limited circumstances and won't usually be relevant to law enforcement data. When we do require consent, we will explain clearly what we are asking for and how we will use it. Consent must be freely given, specific and informed and there must be a genuine choice about offering your data. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

If we have asked you to provide your consent in order to process your personal data, you also have the right to withdraw your consent at any time. When we ask for your consent, we will tell you how we will process your data, how long we will keep it for and the steps we will take to delete it. We will also outline the steps we will take if you decide to withdraw consent.

Withdrawing your consent will be as easy as it was when you gave it. Where possible you will be able to withdraw your consent using the same method as when you provided it. By withdrawing your consent to processing this will be done without you suffering any detrimental effect.

11. How long do we keep personal data?

Occasionally, where there are no other appropriate grounds, the Met may ask for your explicit consent in order to lawfully process your data. This will only happen in specific and limited circumstances and won't usually be relevant to law enforcement data. When we do require consent, we will explain clearly what we are asking for and how we will use it. Consent must be freely given, specific and informed and there must be a genuine choice about offering your data. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

If we have asked you to provide your consent in order to process your personal data, you also have the right to withdraw your consent at any time. When we ask for your consent, we will tell you how we will process your data, how long we will keep it for and the steps we will take to delete it. We will also outline the steps we will take if you decide to withdraw consent.

The Met retains data in line with the Met's retention policy [and in accordance with the Management of Police Information -

<https://www.app.college.police.uk/app-content/information-management/management-of-police-information/> taking into account the type, content and sensitivity of the data, related records, the purposes for which we process your personal data, and any legal or business requirements. Personal data will be retained for as long as necessary for the particular purpose or purposes for which it is held.

12. Who will we share data with?

The sharing of data is a primary business function. For example, it may be necessary to share data with other law enforcement agencies, both nationally and internationally, and with partner agencies working on crime reduction and prevention initiatives. We may also share data with a range of other bodies such as the press and media, service providers, current, past and prospective employers, voluntary sector organisations, financial institutions and regulatory bodies.

The Met takes steps to ensure that any disclosures of personal data, however obtained, comply with the provisions of the Data Protection Act 2018 and General Data Protection Regulation. This includes ensuring that any disclosures are necessary and proportionate. Disclosures will be made on a case-by-case basis, using the personal data appropriate to a specific purpose, and with necessary safeguards in place.

Some of the bodies or individuals to which we may disclose personal information are situated outside of the European Union (EU). If we do transfer personal data to outside of the EU, we undertake to ensure that there are appropriate safeguards in place to certify that it is adequately protected as required by the legislation.

We will also disclose personal information to other bodies or individuals when required to do so by, or under, any act of legislation, by any rule of law, and by court order.

13. How do we keep your data secure?

Your personal data will be processed securely. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, contractors and other third parties who have a business need to know - They will only process your personal information on our instructions.

14. Is my data subject to automated decision making or profiling?

No, you will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

15. Your rights as a data subject

Under the Data Protection Act 2018 you have a number of rights that you can exercise in relation to the data we process about you. Under certain circumstances, by law you have the right to:

- request access to your personal information (commonly known as a right of access request). This enables you to receive a copy of the personal information we hold about you and check that we are lawfully processing it and that it is accurate
- request rectification of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected
- request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no lawful reason for us to continue to process it
- request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we are allowed under the law to charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we can refuse to comply with the request in such circumstances.

We sometimes need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Further information about these rights can be found within the Data Protection Act 2018 and on the Information Commissioner's Office website: www.ico.org.uk

To exercise any of these rights please contact the Information Rights Unit at: DPAMailbox-ROAR@met.police.uk

Or via:

MPS Information Rights
Unit
PO Box 313
Sidcup
DA15 OHH

16. Complaints and further queries

The Met tries to meet the highest standards when processing personal data. We take complaints very seriously. If you have any concerns about the way that we have handled

your personal data please bring it to our attention via the following means:

MPS Information Rights Unit
PO Box 313
Sidcup
DA15 OHH

You are also able to submit complaints to the Information Commissioner's Office, advice on how to contact them based on the nature of your concern is available at <https://ico.org.uk/concerns/>