METROPOLITAN POLICE Working together for a safer London

Freedom of Information Act Publication Scheme	
Protective Marking	Not Protectively Marked
Publication Scheme Y/N	Yes ☒ No☐
Title	Data Protection Act 1998 (DPA) Compliance Standard Operating Procedure (SOPs).
Version	1
Summary	The purpose of this document is to define the minimum standard operating procedures to be applied by Metropolitan Police Service (MPS) personnel in order to support compliance with the DPA 1998.
Branch / OCU	Security, Standards and Architecture
Date created	March 2011
Review date	March 2014

.

Processes for Data Protection Act 1998 Compliance - Standard Operating Procedures (SOPs)

Table of Contents

1.0 INTRODUCTION

These SOPs form part of the MPS Information Management Policy. They are designed primarily to ensure that all MPS personnel and where appropriate our partners, fully understand their duties under the Data Protection Act 1998 (DPA).

Due to the nature of police work, the Metropolitan Police Service (MPS) everyday processes significant quantities of personal and sensitive personal data. This can relate to a wide range of data subjects including persons, who are for instance victims, witnesses and suspects in relation to crime or other core policing activities. Personal data is also collected and processed regarding our police officers, police staff and volunteers etc. and used for staff and other administrative purposes.

The data we process is governed by various pieces of legislation; the most important including the Data Protection Act 1998 (DPA), Human Rights Act 1998 (HRA), the Freedom of Information Act 2000 (FoIA) and the Common Law Duty of Confidence.

In particular the DPA is designed to directly protect such personal information and to ensure that it is handled fairly and lawfully. It provides individuals that are data subjects with legal safeguards and redress regarding their fundamental rights and freedoms. The DPA also sets out how such information will be held and used by organisations, such as the MPS that controls and/or processes personal data.

Our ability to value, protect and process this information fairly and lawfully directly impacts the level of confidence and trust that members of the public have in the police service. Failure to provide this basic level of protection is likely to erode the trust required to operate an effective service, damage the MPS reputation and lead to sanctions imposed by the Information Commissioner's Office (ICO) or through court action.

Some aspects of these SOPs are by their nature complex so a quick-reference overview of the DPA is provided in **Appendix A** to assist readers.

This guidance is created in line with the ACPO Data Protection Manual of Guidance (ACPO DP MoG). Therefore, those who require a more detailed and overarching guide are recommended to read the ACPO DPA Manual of Guidance. If this guidance does not cover your particular enquiry please contact the MPS Public Access Office (PAO) for further guidance.

1.1 Purpose

This Standard Operating Procedures (SOP) is created to guide police officers and police staff of all ranks/grades through the requirements of the Data Protection Act 1998 (DPA or 'the Act').

Where the SOPs touch on other legislation/case law or other MPS processes, personnel are advised to additionally refer to the appropriate SOPs, other subject specific guidance or expertise for a fully informed view, preferably in advance of contacting the Public Access Office (PAO).

1.2 Scope

These SOPs describe in detail what is required to allow personal data to be processed in accordance with the DPA. The central tenet is that processing of personal data must be carried out legally in accordance with DPA Principles 1 to 8 (as set out in sections 7 to 15 of this SOP) and in line with our notifications to the Information Commissioner's Office (ICO) (see section 9.1). The additional SOPs relating to Information Sharing (see section 17) and International transfers of personal data (see section 15) should also be consulted as required and supplement the advice in this SOP.

It is important that personal and sensitive personal data is appropriately valued by the MPS and the key to achieving this is protective marking. Application of appropriate classification of personal data using the Protective Marking System (PMS) identifies the security measures necessary to achieve this aim. The METSEC Code (MPS Security Manual) GEN1 Protective

Marking System (PMS) provides full guidance on protective marking and helps ensure that Principle 7 of the Act is fulfilled (see also section 14).

2.0 APPLICATION

All police officers and police staff, including the extended police family and those working voluntarily or under contract to the MPA must be aware of, and are required to comply with, all relevant MPS policy and associated procedures.

However, this SOP applies in particular to officers and staff in the following roles, ranks or grades:

- Borough Operational Command Unit (BOCU) commanders
- OCU commanders
- Heads of branches
- Other managers and supervisors
- DoI2 (3-3) Public Access Office personnel, including the Data Protection Officer (DPO)
- Other MPS personnel who handle information during the course of their duties; and
- Any other MPS personnel, such as front counter staff, responsible for contact with the public

N.B. This list is not intended to be exhaustive.

These SOPs have a wide application and relevance to policing activities. They apply in particular to officers and staff who have defined responsibilities for ensuring that they and their personnel are appropriately briefed on data protection legislation and the recording, processing and sharing of personal/sensitive personal data in accordance with policing purposes.

3.0 ROLES AND FUNCTIONS

There is an expectation that all persons handling personal data have a basic understanding of the main provisions of the Act and can correctly recognise what does and does not constitute personal and sensitive personal data (see sections 4 and 5). All personnel handling personal or sensitive personal data **must** exercise due diligence and care in its collection, processing, use, movement, storage and disposal. It should be remembered that ignorance of the law is no excuse so it is important that readers familiarise themselves with the provisions in these SOPs.

Additionally, managers and supervisors throughout the organisation need a sufficient awareness of the main DPA issues, how they impact on their processes and enable them to

assist and train their staff. This section provides details of the specialist help and advice available to the organisation from the Public Access Office.

The leading MPS information governance roles are detailed within the MPS Information Governance Framework (IGF) document. In addition to the IGF the main roles outlined within this framework are as follows:

3.1 The Head of the Public Access Office

- In addition to the role defined within the Information Governance Framework, the Head of the Public Access Office (PAO) role assumes the title of Data Protection Officer (DPO) in relation to the DPA on behalf of the Commissioner of Police for the Metropolis.
- The Head of Public Access Office also assumes the role as the MPS ACPO Representative and the ACPO South East Region FoIA Representative on the National ACPO Data Protection, Freedom of Information and Records Management Group, and the ACPO South East Region Data Protection and Freedom of Information Group.
- The Head of Public Access Office is the Single Point of Contact for communications made on behalf of the Commissioner of Police for the Metropolis between partner agencies and the Information Commissioner's Office on all matters relating to the DPA.

3.2 The Deputy Data Protection Officer (Deputy Head of the Public Access Office)

- Assists the Data Protection Officer in managing the Commissioner's statutory responsibilities under the DPA;
- Provides senior decision maker guidance on legislative and policy compliance to all areas of the MPS;
- Monitors all MPS and Public Access Office performance against Corporate Health Check Indicators and taking necessary action where there are areas of poor performance/non-compliance with the DPA;
- Is the secondary leading liaison point within the MPS for ACPO members, partnership agencies and the Information Commissioner's Office (ICO) on DPA legislation matters;
- Implements and maintains DPA complaint and ICO complaint management within the PAO; and

- In the absence of the Data Protection Officer, provides MPS representations at the ACPO National and Regional FoIA Portfolio Group Meetings in order to raise, discuss, debate issues of national/regional interest, which contributes to the overall development of national policy or action.

3.3 The Information Sharing Unit, Senior Advisor

- Working directly to the Head of the Public Access Office, the Information Sharing Support Unit (ISSU) Senior Advisor is responsible for ensuring that MPS information is shared safely and within corporate information sharing rules.

3.4 The Data Protection Higher Information Access Manager

- Handles all ICO DPA Complaints;
- Leads dedicated teams of PAO DPA caseworkers;
- Provides higher DPA support to all areas of the MPS in regards to legislation, policy and process;
- Assists with or further escalates issues, which are causing persistent DPA non-compliance and high-risk issues/cases for DPA;
- Reviews and reports on all statistical analysis created by the PAO/FoIA Support Officers;
- Ensures that the PAO DPA caseworkers follow all relevant DPA SOPs, processes and policies;
- Ensures that the PAO DPA caseworkers are equipped and trained to complete subject access requested under the DPA and limited DPA advice; and
- Is the higher conduit for information/guidance between the PAO and other areas of the MPS.

3.5 The Data Protection Casework Manager (Triage and Complex teams)

- Manages DPA subject access teams;
- Processes high level subject access requests;
- Completion of DPA complaints re: accuracy, the Police National Computer (PNC) and Subject Access Requests (SAR) process; and
- Provides DPA advice and guidance where appropriate.

3.6 The Data Protection Caseworker

- Completes subject access requests (SARs); and
- Provides low level DPA advice and guidance regarding SARs.

4. 0 WHAT IS PERSONAL DATA?

Personal data is data relating to an identifiable living individual, which includes (but is not limited to) expressions of opinion, biographical information and decisions to be or that are made about the individual or in respect of the individual.

What is defined as personal data is wide and has been subject to considerable debate. However, it is advisable to note that whilst some information the MPS receives may not be personal data to the person or organisation which transferred or shared the information with the MPS, it is likely that this information becomes personal once in our possession due to the likelihood of being able to identify the individual through our systems, data and processes.

For Example: Information is received via a sharing agreement with another agency that gives the given name of the partner of a subject. Within systems held within the MPS we are able to categorically identify that person by a combination of the shared information and what we already hold. The given name then becomes personal information; it may well become sensitive personal information dependent on the links established.

Personal data includes (but is not limited to):

- Human Resources (HR) records;
- Meeting minutes regarding an individual (such as Multi-Agency Public Protection Arrangements [MAPPA] minutes, Occupational Health [OH] records, case conferences etc.);
- Management performance reports;
- Pocket notebooks;
- Closed Circuit Television (CCTV) imagery;
- Interview records;
- Completed examination scripts;
- References;
- Fingerprints;
- DNA information;
- System entries such as the Crime Intelligence System (CRIMINT PLUS), Police National Database (PND) and Police National Computer (PNC) etc records;
- Vehicle Registration Mark (VRM) details;
- Staff contact lists; and
- Flexible working time sheets.

Some categories of personal data are given a higher degree of protection under the Act and are defined as 'Sensitive Personal Data' (see section 5).

5.0 WHAT IS SENSITIVE PERSONAL DATA?

Sensitive Personal Data is personal data consisting of the following information regarding the data subject:

(a) Their racial or ethnic origin;
(b) Their political opinions;
(c) Their religious beliefs or other beliefs of a similar nature;
(d) Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations [Consolidation] Act 1992);
(e) Their physical or mental health or condition;
(f) Their sexual life;
(g) The commission or alleged commission by the data subject of any offence; or
(h) Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

The very nature of policing will require the processing of large amounts of sensitive personal data regarding a number of individuals who come into contact with the Service in one form or another. To process this information fairly and lawfully there are additional conditions within the Act which must be met. This is covered in section 8.5.

6.0 WHAT IS DATA PROCESSING?

The Act defines data processing as:

- Obtaining, recording, holding, organisation, adaptation, alteration, retrieval, consultation, alignment, combination, blocking, erasure, destruction, disclosure, transmission, dissemination, or otherwise making available the data or information.

As can be seen from the above list the processing of data can take many forms, e.g. an entry on the Stops Register giving details of a specific person, amounts to data processing.

6.1 What is a Data Controller?

A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

For example, the MPS Commissioner determines the 'how, what, when, why and where' rules around the personal data in which the MPS processes. Therefore, he is the Data Controller for the MPS. The Commissioner takes the overall responsibility for whatever happens to the data processed by the MPS, therefore, is liable for breaches of the Act, certain criminal offences, civil proceedings and Information Commissioner's Office enforcement action. Those working for the MPS must be aware of the requirements of the Act on them as data processors, and their liabilities including criminal offences contained within this and associated Acts. In certain circumstances the Commissioner takes on the role of 'data controller in common' or 'joint data controller'. Such circumstances derive out of data processing arrangements where there is more than one data controller which determines the rules/processes etc of the data processed. An example of this is PNC. Each Chief Constable decides the what, when, why, how & who regarding the data his/her force uploads onto the PNC and follows the PNC national guidelines and policy which is set and agreed by each Chief Constable. Each Chief Constable takes responsibility for the data their force uploads onto the PNC.

6.2 What is a Data Processor?

A person [other than an employee of the data controller] who processes the data on behalf of the data controller.

For example, the MPS has outsourced its pay and pensions processing to a service provider. This service provider processes the personal data of MPS employees on behalf of the Commissioner of Police of the Metropolis, however, does not determine the 'how, what, when, why and where' rules (as above) as the service provider follows the rules set by the Commissioner. Therefore, the service provider is deemed to be a Data Processor.

If the data is being transferred to a Data Processor a Data Processing Agreement will need to be established. Business Groups **must** seek the advice of the (Deputy) Data Protection Officer before embarking on the creation of a Data Processing Agreement as templates are already established and held by the PAO. Business Groups should note that the Commissioner of Police of the Metropolis is still legally responsible for making sure that the data is processed in line with the Data Protection Act 1998 principles. In particular, personal data can only be transferred if there is a contract requiring the processor to have appropriate security and act only on MPS instruction. The personal data should continue to be protected to the same standard as in the UK which includes the protection of the rights and freedoms of

data subjects. When selecting a processor, Business Groups need to satisfy themselves that it is reliable and has appropriate security [as will be advised /accredited by the Information Assurance Team].

If the intention is to use a Data Processor outside of the UK Business Groups must follow the advice contained within the Data Protection Act 1998 (DPA) Compliance Standard for International Data Processing Standard Operating Procedures (SOPs) and seek the advice of the (Deputy) Data Protection Officer.

7.0 THE DATA PROTECTION ACT 1998 PRINCIPLES

The Data Protection Act 1998 (DPA) has eight key principles which underpin the legislation. The Commissioner **must** comply with these principles when processing personal data and they are listed as follows:

Principle 1 - The data **must** be processed fairly and lawfully.

Principle 2 - The data obtained and processed **must** be in line with a specified and lawful purpose.

Principle 3 - The data **must** be adequate, relevant and not excessive in relation to the purposes in which it was collected.

Principle 4 - The data **must** be accurate and kept up to date.

Principle 5 - The data **must** not be kept longer than is necessary for the purposes in which it was collected.

Principle 6 - The data **must** be processed in accordance with the rights of data subjects under the Act.

Principle 7 - Appropriate technical and organisational measures **must** be taken against unauthorised or unlawful processing of personal data and against loss, destruction or damage to the data.

Principle 8 - Personal data **must** not be transferred to a country or territory outside the European Economic Area (EEA) unless that country of territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The following chapters of these SOPs will be headed by the appropriate principle to enable users to review relevant sections so all personal information processing meets the requirements of the Act.

8.0 PRINCIPLE 1 – FAIR AND LAWFUL PROCESSING

Sections 4 and 5 above detailed what is defined as personal and sensitive personal information. Principle 1 determines that in processing this information the MPS must meet the following criteria:

1 Be Fair

2 Be Lawful

3 In the case of processing personal data, meet at least one condition in Schedule 2.

4 In the case of processing sensitive personal data, meet at least one condition in Schedule 2 and one Condition in Schedule 3.

8.1 HOW TO ENSURE THAT THE PROCESSING IS FAIR

In order to meet the fairness requirements under the DPA the MPS completes a number of activities to ensure the data we process is obtained and used fairly. In particular this is via the use of fair processing notices in custody suites and front offices across MPS sites together with a copy available to data subjects on the MPS internet site. Where applicable the MPS will also inform individuals of the way information will be used when it is obtained via particular forms.

In order for processing to be fair the MPS must have legitimate grounds for obtaining and using information, while also being transparent about the way the data will be processed. As is the practice in other organisations there is a requirement to inform individuals about the way their data will be handled. It is understood that this is not normally a practical approach for the MPS i.e. when dealing with the arrest of a suspect or assisting with a distraught victim, so the MPS provides clarification of the way data is handled with the use of a fair processing notice.

To comply with the fairness element of the DPA public authorities are expected to ensure that they meet the legitimate expectation of individuals when processing their data. In respect of any crime information there is a general expectation by the public that information provided to police will be used in support of legitimate policing purposes. The same considerations apply with regard to the HR information held on an individual where the expectation is that information is used in regard to their management, pay, welfare etc. during service with the MPS.

8.2 FAIR PROCESSING NOTICE

As mentioned above the MPS makes use of a fair processing notice to ensure compliance with the Fair element of the DPA. **This document must be on display in all front offices and custody suites to ensure the MPS is compliant with the Act.**

MPS Fair Processing Notice:

http://www.met.police.uk/foi/pdfs/other_information/corporate/mps_fair_processing_notice.pdf

A form of words has also been compiled for use on MPS forms where a fair processing notice is required during the collection of data from individuals. An example can be found at **Appendix C**. This text is currently used on the **MPS corporate form 696** which can be accessed at Promotion Event Risk Assessment Form.

8.3 SCHEDULE 2 CONDITIONS

In order to lawfully process any **personal data** the MPS needs to satisfy at least one Condition in Schedule 2 of the Act. The Schedule 2 Conditions are as follows:

(1) **Consent has been given by the data subject** - MPS view on the use of consent is detailed below;

(2) **It is for entering or performing a contract with the data subject** - this is unlikely to be utilised by the MPS as it requires a contact direct with individual data subjects;

(3) **The data controller is under a legal obligation, other than under contract** - This is used on occasion where the MPS is legally obliged to provide information, this may include certain information released in relation to employment records;

(4) **It is to protect the vital interests (life or death interests) of the data subject** - This element can only be relied upon in purely life of death situations i.e. personal information must be shared with medical staff to ensure the survival of an individual;

(5) **It is for the administration of justice, exercising functions under an enactment, exercising of government functions, or the exercise of any other functions of a public nature in the public interest** - This element allows information to be processed where a power is provided under a specific law i.e. Section 115 of the Crime and Disorder Act 1998 that allows information sharing between specified crime and disorder partners in support of the requirements of the Act; and

(6) **It is for the pursuit of the legitimate interests of the data controller** - This provision provides the ability to process information in the main for the MPS i.e. where a police officer is using or obtaining information under their common law powers to investigate the prevention or detection of crime which would be judged the legitimate aims of the MPS.

8.4 CONSENT

Whilst the obtaining of consent is listed as one of the Conditions which would deem the processing lawful the MPS does not rely on consent alone. This is because consent can be withdrawn by the individual at anytime, rendering the continued processing of the information unlawful, unless it is supported by another relevant Condition. There are limited circumstances where consent is safe and appropriate to rely upon as a Condition e.g. the collation of Ward Panel names and addresses by safer neighbourhood teams. However, as required by the Act Principles, local processing practices must have the ability to amend or delete records where the consent to retain this information is withdrawn.

8.5 SCHEDULE 3 CONDITONS

In order to lawfully process **sensitive personal information** the MPS needs to satisfy at least one Condition in Schedule 2 together with at least one Condition in Schedule 3 of the Act.

(1) **Explicit consent has been given by the data subject** - As stated above the use of consent is rarely proceeded with by the MPS. In the case of sensitive personal data the consent would have to be specific, clear and unambiguous;

(2) **It is for the exercise of rights or obligations in connection with employment** - involved information processed in accordance with employment law;

(3) **It is to protect the vital interests (life or death interests) of the data subject or anyone else** - as per the Schedule 2 condition this involves information disclosed in life or death scenarios. The addition of the text ‘anyone else’ covers scenarios such as confirmation of the HIV status of an individual in custody where medical staff are dealing with an open wound and the information has not been forthcoming from the suspect;

(4) **It is part of the legitimate activity of a not for profit organisation** - This is not applicable to the MPS;

(5) **The personal data have already been made public by the data subject** - Unlikely to affect the MPS;

(6) **It forms part of legal proceedings, including obtaining legal advice, and exercising or defending legal rights** - This covers the MPS requests for legal advice via DLS or external counsel involved in civil actions on behalf or against the MPS; and it will also cover the release of information to the CPS and external counsel in the course of criminal proceedings;

(7) **It is for the administration of justice, or exercising functions under an enactment, or exercising of government functions** - This element allows information to be processed where a power is provided under a specific law i.e. Section 115 of the Crime and Disorder Act 1998 that allows information sharing between specified crime and disorder partners in support of the requirements of the Act;

(8) **It is for medical purposes** - This form of processing can only be relied upon by a medical professional;

(9) **It is for the purpose of monitoring equality of opportunity** - specifically relates to requirements on the MPS to record and report on equality information; and

(10) **The Act also allows for the Secretary of State to make an Order providing other conditions which allows the processing of sensitive personal data** - one notable and relevant Statutory Instrument (SI) is SI417/2000, The Data Protection (Processing of Sensitive Personal Data) Order 2000, which provides the following condition:

The processing is necessary for the functions conferred on (required of) a constable by any rule of law.

The above SI covers "*any rule of law*" conferred on a constable which includes common law. Whilst statute law may not cover specifically the data processing requirements needed, common law powers may do so in specific circumstances. For further guidance on the application of SI417/2000 please contact the Public Access Office.

8.6 HOW TO ENSURE THAT THE PROCESSING IS LAWFUL

In accordance with principle 1, any processing of personal data must be allowed by, or required by, statute or common law. In practice for the MPS this will encompass the statutory legal powers we have under legislation to obtain and process information i.e. the powers to take DNA and fingerprints of all people detained at a police station under the Police & Criminal Evidence Act 1984 (PACE). Since 2005 the Service is also able to rely upon the

'police information' processed under policing purposes which are defined in the statutory Code of Practice on the Management of Police Information (MoPI) as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice; and
- Any duty or responsibility arising from common or statute law.

These core policing purposes reflect the wide use of personal data within the MPS. **This means that if your handling of personal data does not meet a policing purpose or a statutory requirement this must be raised with the Data Protection Officer (DPO) immediately.** In order for the MPS to lawfully process personal data any specific legal requirements must be fulfilled. This requires consideration of the following:

- **The Common Law Duty of Confidence** - The duty of confidence arises where an individual confides with another and passes information with the intention it will only be used in accordance with their wishes. Within the MPS the majority of information obtained this way will be in respect of the prevention and detection of crime. There will be an expectation that the information will be used in support of that particular purpose. The duty of confidence may arise in police specific circumstances i.e. in relation to the handling of informant information. In such cases robust data handling processes are in place to handle the management of information. The Duty of Confidence can be overridden by a legal obligation, the specific consent of the individual and where the processing would be defined as being in the public interest. For example, where information is required to prevent the commission of offences or to safeguard children.
- **HRA Article 8 rights to Respect for Private and Family Life, Home and Correspondence** - This right is not absolute and information can be processed where:
    - it is in support of a legitimate aim (i.e. prevention and detection of crime);
    - proportionate (the process needs to be done and only the limited amount of information is taken and used); and
    - it is appropriate and necessary in a democratic society (the processing benefits the majority of the public).

<u>Privacy Impact Assessments</u>

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. PIAs in particular highlight:

- privacy risks to individuals;
- privacy and DP compliance liabilities of the MPS; and
- reputation risks to the MPS.

Within the MPS PIAs should only be undertaken on projects if it is felt that there is high risk to the MPS of the processing of personal data resulting in a high impact risk as detailed above. Consultation with the PAO regarding PIAs should be sought prior to the commencement of projects.

9.0 PRINCIPLE 2 – PROCESSED FOR LIMITED PURPOSES

The DPA requires that information is obtained for specified and lawful purposes. This principle links directly to Principle 1 detailed above, as the fair processing and lawful elements support the data controller in meeting this principle.

The Act requires that information is processed for one or more specified purposes and that this is communicated to the data subject during collection. This data will then be processed in accordance with those purposes and not passed to any other organisations for processing outside of those purposes unless there are statutory or common law requirements to do so. Further guidance on lawful data processing can be obtained from the Public Access Office.

In the case of the MPS the majority of personal data is obtained and processed in accordance with policing purposes. Where information is processed in support of policing purposes then this principle is met. With regard to other data the same principle applies; for example HR data will be used for HR related activities. The MPS informs the public together with officers and staff via the notification requirements detailed below.

9.1 NOTIFICATION

The Act makes it a lawful requirement for all organisations (not subject to an exemption) to notify to the Information Commissioner (ICO) the details of the personal data processed by the data controller. Failure to do so is a criminal offence under Section 21 of the Act.

Currently there are four purposes notified to the ICO for the MPS to control and process personal and sensitive personal data. These are as follows:

- Staff Administration;
- Policing;
- Administration and ancillary support for policing purpose; and
- National Security.

The intention of the notification process is to aid transparency around what data we process, why, how and with whom we intend to disclose the information and where located. It is not intended to be an exhaustive list as this is usually not practical, but the notification must provide sufficient detail as to the overall picture of our processing.

The registration of the MPS notification (including any amendments) to the ICO is made by the Data Protection Officer (DPO). The MPS registration is publicly available on the ICO website which can be found at: Data Protection Public Register and by entering the registration no: Z4888193.

Important Note - If you or your Department are undertaking a project or initiative which involves a new type of processing of personal data then you **must** inform the Data Protection Officer (DPO). The DPO will undertake a Data Protection assessment, which will include a consideration as to whether the MPS registered notification entry covers the required processing. **Failure to do so may place the MPS Commissioner in breach of the Act and liable for a criminal offence**.

10.0 PRINCIPLE 3 – ADEQUATE, RELEVANT AND NOT EXCESSIVE

To ensure that information is appropriately managed the DPA requires specifically that information is fit for purpose and collection is sufficient to meet the intended purpose. Excessive processing of information for the sake of holding information should be avoided where possible. Although this might be difficult in the area of live investigations consideration should however be made as to what information is sought and subsequently retained.

11. PRINCIPLE 4 – ACCURATE AND UP TO DATE

The DPA requires that personal information is accurate and where necessary kept up to date. All officers and staff should make every effort to ensure that information is recorded accurately. This should include the notification of any source of the information where appropriate, i.e. such a process is automatically available within CRIMINT. Where information is recorded as an opinion, either by a member of the MPS or from a victim or suspect, it should be recorded in such a manner to identify that this is the case. Where the accuracy of information is challenged by the subject such a complaint will normally be handled by the PAO. **Please note that records may need to be amended or an addition recorded subsequent to the PAO review of the complaint which will need to be facilitated by the Officer in the Case (OIC).**

In regard to the requirement to keep information up to date, much of the information held by the MPS are historic records i.e. of an event, crime, intelligence report or as a snap-shot of a particular period in time. In such circumstances there is no requirement for the original record to be amended i.e. where a change of address or circumstances have been notified. It is, however, important that where appropriate, records are added to or person (nominal) records amended where new information comes to light. In the case of the PNC where individuals come to notice address details should be amended accordingly; however the previous address details will also be retained in order to support any later investigations linked to that address.

12.0 PRINCIPLE 5 – NOT KEPT FOR LONGER THAN IS NECESSARY

This principle seeks to ensure that information is retained as long as the purpose for which it was obtained remains, and for no longer. Within the MPS, Records Management Branch (RMB) is tasked with providing the specific review and destruction periods for the information we hold.

The current retention schedule can be viewed at: MPS Records Management - Retention and Disposal of Records. The retention of information is determined by a number of factors such as relevant legislation including the Public Records Acts together with judicial rulings and government guidance.

13.0 PRINCIPLE 6 – PROCESSED IN ACCORDANCE WITH THE RIGHTS OF THE DATA SUBJECT

The DPA provides data subjects with six rights in accordance with the Act and the way their data is processed.

13.1 The Right of Access to Personal Data (Section 7)

Requests from individuals to access their own personal data are referred to by the Act as **'Subject Access Requests' (SARs)**. The Public Access Office (PAO) processes all requests made by members of the public or their representatives to access MPS held data. *However*, requests made under PACE or for legal proceedings (criminal or civil) do not fall under the PAO remit; as such requests are not deemed to be SARs.

Important Note:

All SARs, including the accompanying ID and fee (where included) must be forwarded to the Public Access Office (PAO) within 48 hours as the organisation has only 40 calendar days to process and dispatch the requested information. If the request requires copies of data held in the receiving location then this must also be forwarded to the PAO for processing.

If a member of the public or their representative seeks to access their personal data under the Data Protection Act 1998 they **must** be advised to complete **corporate form number 3019**, see the link at MPS Corporate Forms Index and follow the guidance contained within that form. Front counter staff at police stations **must** be prepared to assist any requester in completing this form, especially where there is a disability or language support requirement. If guidance in this regard is needed staff are advised to contact the Public Access Office for further assistance.

The MPS will endeavour to meet the reasonable and proportionate needs of individual requestors in order to remove any barriers to accessing information; to generally make the process as accessible as possible to all sections of the community and to encourage active participation in public life. To meet this duty, MPS personnel **must**:

- **Take care not to discourage requestors from making legitimate requests;**
- **To be sensitive when dealing with individual needs; and**
- **To do their best to help requestors submit subject access requests**.

The extent of any advice and assistance provided will always be subject to the availability of appropriate MPS resources.

The following persons have been identified as potentially needing special requirements in this area:

- **Where age is a factor** - young children with limited understanding and older persons exhibiting infirmity may require additional assistance;
- **Disabilities or impairments (physical, mental or learning)** - a large range of persons requiring different types of help, including the blind/visually impaired and persons with deafness; and
- **Information requests submitted in a language other than English (or Welsh)** - or where a request is received to translate the information to be supplied into another language.

13.1.1 Where age is a factor - Ideally, children and older persons will be assisted by a personal representative best able to understand their individual needs and to help with putting in a written request for subject access on their behalf. For unaccompanied children or older persons attending a police station, it may be necessary for MPS personnel to help set out and record the request in writing with their agreement. The subject access right will provide the information to a third party only where the **explicit** consent of the subject has been received, unless the request is from a child under 12 years of age or where there is power of attorney (or other evidence), as detailed below.

13.1.2 Disabilities (as defined in the Equality Act 2010) or other impairments (i.e. physical, mental or learning) - This can act as a barrier for requestors wishing to access information. This is particularly so if requestors attend police stations and there are communication barriers (e.g. maybe due to visual impairment or deafness etc.). Requestors may also be unable independently to write down exactly what they require from their subject access request. Again the assistance of a personal representative for the requestor is invaluable, but where such a person is not present further assistance should be provided either by front counter staff or via the PAO customer services.

13.1.3 Information requests received in a language other than English or Welsh - People who speak little or no English may attend police stations or written requests maybe received in a language other than English. They are likely to require help to interpret and translate their meaning or generally with communicating their information needs. Ideally, such help will initially come from their personal representative (e.g. friend/ relative) or a known contact within the local community. In all these situations, the MPS will endeavour to assist in order to best meet the reasonable and proportionate needs of requestors.

13.1.4 Requests to provide information in a particular format or language other than English or Welsh - There is no requirement for the MPS to process requests received in another language (i.e. not English or Welsh), or the supply of data is also requested in another language as this is likely to meet the conditions of a disproportionate effort as defined in Section 8 of the Act. Where an applicant makes a request in a language other than English (or Welsh), the MPS will inform the applicant, in English that a request must be made in either English or Welsh. If there are any remaining doubts as to how to respond to requestors in these circumstances, such matters should be discussed with the Public Access Office as soon as possible.

Important Note:

Front office staff responsibilities (as listed above), is with regard only to the assistance of individuals wishing to make a subject access request. Front office staff must not physically accept requests and the applicant must be advised to send their completed request with associated fee and identification documentation direct to the Public Access Office.

The PAO hold separate internal SOPs in regard to the processing and management of SARs. The processing requires a number of considerations over the information requested and held by the MPS in accordance with the right of the data subject, any exemptions that may be relevant to a particular case and the requirement to protect information related to third parties.

MPS personnel (Officers and staff) are advised that their details may be released under a subject access request. Advice from the ICO states that third party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual. For example, the name of an investigating officer that has had direct contact with a victim would see their name released if that victim sought access to the relevant crime report.

The PAO processes all requests as an independent unit within the MPS to ensure that there is ‘an arms length’ approach to deal with each case individually and by applying appropriate knowledge and skills to interpret the requirements of the Act. Where cases are complex and a relevant officer/staff member can be identified an opportunity to confirm the release of any intended disclosure will be provided. Where required a copy of the intended disclosure can be provided for consideration prior to release, however any feedback will need to be **prompt**

and within the 40 day timescale for completion of cases. **The decision of the Data Protection Officer (DPO) will be final in regard to any disputed disclosures.**

Important Note:

Upon receipt of a request the PAO will locate the requested information and require urgent dispatch of a full, unedited copy of the original record within 48 hours. Failure of any OCU or BOCU to supply data on request of a PAO DPA Caseworker potentially places the MPS Commissioner in breach of the Act and such instances will, therefore, be escalated accordingly.

13.1.5 Requests Made by Representatives or Parents or Guardians - A data subject may chose to use a representative to submit their SAR to the MPS on their behalf. In order to ensure that the data subject is in full knowledge and provides explicit consent of this request being submitted on their behalf the PAO will only process such requests when in receipt of a written and signed letter of authority. Where consent cannot be obtained (due to disability reasons, for example) a copy of the Power of Attorney (or other evidence) will be required as evidence of the representative acting in the data subject's interests and on their behalf.

Requests made on behalf of children by their parents or guardians can only be submitted by those who have legal custody of the child and where the child is under the age of 12. Children over the age of 12 are considered to be of mature mind to make an informed judgement as to whether they wish to exercise their rights under the Act. Therefore, if a request is received by a parent of a child 12 years of age and over they will be required to supply a signed letter of authority by the child.

13.1.6 CCTV Requests - Members of the public or their representatives, as detailed above, may request access to CCTV footage held by the MPS. Providing a copy of CCTV footage is very costly to produce where there are third parties shown in the requested footage. If the CCTV footage is solely of the requester (and no third party imagery is included) then a full copy may be provided to the applicant (subject to individual case assessment and relevant exemptions). In instances where the footage includes identifiable third party imagery an assessment will be made as to the risk of providing a supervised view only access of the footage to the requester. Such assessment will be made in consultation with the Officer in the Case (OIC) and with the authority of the PAO DPA Higher Information Access Manager.

Once approved by the PAO, the (B)OCU will arrange a supervised viewing session for the applicant to attend locally either alone or with their representative (e.g. their solicitor). Such arrangements must be made in a reasonable time period and no later than the 40th calendar day of receipt of the request (unless specifically requested by the applicant to extend this period). Only one viewing session is provided per request. Repeat requests **must** be submitted as a new request and will be assessed for reasonableness by the PAO.

13.1.7 Requests Made by Officers and Staff (MPS personnel) - It should be realised that officers and staff are equally entitled to make data subject access requests (SARs) in their private capacity. Also police officers have a right to inspect their personal record under Regulation 15 of the Police Regulations 2003.

Members of staff are advised in the first instance to approach their local line manager or Human Resources (HR) for access to MPS held personal information. Managers who receive such requests **must** treat all requests fairly without threat (directly or indirectly) of disciplinary action or unfair disadvantage as a result of making such a request. Staff should be reminded of the information available directly to them via the HR self service system if this is sufficient to meet their request.

Requests **must** be completed in a timely fashion and access given **no later than the 40th calendar day** from the request being made. Where there are complex issues or disclosure concerns managers, HR staff are advised to contact the PAO for advice or consideration of whether the request should be noted as an SAR and dealt with accordingly.

If staff members are concerned with submitting their request locally then they are advised to contact the PAO for further advice.

The PAO DPA Caseworker **must** receive a written letter of authority from the data subject in order to discuss any case with a staff association or legal representative once a SAR has been received. An internal email to this affect will be accepted.

Requests for HR, Occupational Health (OH) or disciplinary information from former officers and staff should be processed under a subject access request. Any individual approaching the service for their records from previous employment within the service should be directed to the subject access process or given the contact details of the Public Access Office. If the request is from the family of a deceased former member of staff please see the guidance at section 18.

13.2 The Right to Prevent Processing Likely to Cause Damage or Distress (Section 10)

Under Section 10 of the Act an individual is entitled, in limited circumstances, to write to the MPS requiring that we do not handle their personal data in a manner that was causing or would be likely to cause unwarranted substantial damage or substantial distress to themselves or another person.

Such requests are separate to those enshrined in PACE 1984 and the Criminal Justice & Police Act 2001, whereby individuals can apply to the MPS Commissioner (via the Serious Crime Directorate) to have their DNA, fingerprints and PNC records deleted following an acquittal at court or any other discontinuance of a case. Such applications **must** be made to the Exceptional Cases Unit at SCD. For further guidance regarding this process please contact the SCD Exceptional Cases & FoIA Unit.

Requests to remove, delete or amend data under Section 10 of the DPA must describe or state the following:

- the personal data involved;
- the handling to which the individual objects;
- state that the handling was causing or would be likely to cause substantial damage or substantial distress to him/ her or another;
- describe that damage or distress;
- state that the damage or distress was/ would be unwarranted; and
- give reasons why the handling was causing/ would cause such distress and was/ would be unwarranted.

All requests of this nature may be sent in writing to the MPS Data Protection Officer (DPO). The DPO has 21 calendar days to investigate and respond to requests; therefore, **all Section 10 requests received by the organisation must be forwarded to the PAO within 48 hours**.

There are exemptions to this right and the PAO will consider these and respond to the applicant accordingly either noting the reasons why the request is unjustified or detailing the extent to which the MPS will comply with the request. Where the MPS refuses a Section 10 request the individual has an opportunity to approach the courts to seek an appropriate order.

13.3 The Right to Prevent Processing for the Purposes of Direct Marketing (Section 11):

Although the MPS does not engage in direct–marketing, under Section 11 of the Act and subject to certain exemptions, an individual has the right to request in writing that an organisation stops within a reasonable time, or does not start, using their personal data for direct marketing purposes. This includes the communication by any means (e.g. mail, email, telephone, door-to-door canvassing) of any advertising or marketing material directed at particular individuals.

Any requests under Section 11 must be forwarded to the MPS Data Protection Officer. Such requests will then be logged in advance of any future use of direct marketing by the MPS. **Due to this requirement it is important that any instances or projects or initiatives involving direct marketing should include a notification to the Data Protection Officer.**

Direct marketing is summarised as any offer to an individual of products or services including the promotion of charitable or political campaigns. Any concerns around the MPS involvement in direct marketing should be raised with the Data Protection Officer.

13.4 Rights in Relation to Automated Decision-Taking (Section 12):

Although the MPS is unlikely to carry out any automated decision-taking that does not involve some human element, under Section 12 of the Act and subject to certain exemptions, an individual has the right to require that the MPS ensures that no decision that would significantly affect them is taken by the MPS or on its behalf purely using automated decision-making software. The right has to be exercised in writing. If there is a human element involved in the decision-making the right does not apply.

Any requests under Section 12 must be forwarded to the MPS Data Protection Officer (DPO). Such requests will then be logged in advance of any future use of automated decision-taking by the MPS. **Due to this requirement it is important that any instances or projects or initiatives involving automated decision-taking should include a notification to the Data Protection Officer.**

13.5 The Right to Compensation (Section 13):

Under Section 13 of the Act any individual who believes they have suffered damage and/or distress as a result of any contravention of the requirements of the Act may be entitled to compensation from the MPS. This is where the Service would be unable to prove that it had

taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

Any claim for compensation arising from this provision of the DPA must initially be discussed with the PAO in order to identify if a complaint case has been received. Where required the request will then be forwarded to the Directorate of Legal Services, Metropolitan Police Service, New Scotland Yard, 10 The Broadway, London, SW1H OBG to advise.

13.6 The Right to Take Action to Rectify, Block, Erase or Destroy Inaccurate Data (Section 14):

Under Section 14 of the Act an individual has the right to seek a court order for the rectification, blocking, erasure or destruction of their inaccurate personal data handled by the MPS. The right cannot be exercised by directing it to the MPS.

13.7 The Right to Request Assessment by the Information Commissioner (Section 42):

Under Section 42 of the Act any person can request the Information Commissioner's Office (ICO) to make an assessment if they believe that they are/ have been adversely affected by the handling of personal data by the MPS. Such requests should be made direct to the Information Commissioner's Office (ICO).

Generally if individuals have any concerns regarding the way their personal data is handled by the MPS or about the quality (accuracy, relevance, excessiveness etc.) of their personal data they are encouraged to raise them with the MPS Data Protection Officer (DPO) in the first instance to formally resolve the issue(s) without the need for ICO involvement.

ALL ICO engagement with the MPS must be forwarded directly to the Data Protection Officer (DPO) for a formal response on behalf of the MPS Commissioner. At no stage must there be any communication made between the ICO and the MPS without engaging the DPO. Failure to adhere to this requirement will be reported directly to the Director of Information.

The ICO additionally provides advice and assistance in regard to individual projects with significant DPA impact. All requests for assistance from the ICO must be filtered through the Data Protection Officer (DPO). This will ensure there is a consistent

approach to develop a repository of ICO advice/ guidance for DPA impacted MPS projects and reduce duplication.

14.0 PRINCIPLE 7 – SECURE

Principle 7 requires the MPS to have appropriate technical and organisational measures against inappropriate use, access or destruction of personal data.

A high standard of care is required by the organisation and all MPS personnel involved with personal or sensitive personal data to ensure that it is protected and held securely at all times. The security area of the Act is covered by the Information Management (IM) Policy published on the Corporate Policy Database, including the provisions to be found in the various information security SOPs and the METSEC Code (MPS Security Manual).

The key to protecting any sensitive information is to first apply protective marking in accordance with **METSEC Code GEN1 - the Protective Marking System (PMS)**. Personal and sensitive personal data should be identified, valued and a protective marking applied when first collected. MPS information records are to be designed, wherever possible to be updated to retain 'one version of the truth' and multiple records and copying of the same information should be kept to a minimum or eliminated. MPS personnel should follow any data quality, data handling and records management requirements plus information management guidance and best practice to ensure personal data always remains protected. Personal data is only ever processed and viewed on a 'need to know' basis. In the MPS, personnel authorised to view and handle personal data are subject to separate security vetting requirements.

Personal and sensitive personal data **must** be held in a secure repository at all times, irrespective of its format (i.e. paper, digital etc.). The preferred storage invariably means inputting the personal data into the corporate system designated for the official purposes for which the data was collected (e.g. CRIS, CRIMINT etc.). All MPS ICT systems **must** undertake a form of security assurance process prior to becoming operational - see **METSEC Code EAA2 Information Assurance**.

Another important aspect is when personal data is stored or processed even temporarily on mobile devices such as laptops, USB pen drives and similar devices. Strict HMG data handling requirements mean that all such devices that potentially could be carried off MPS premises **must** have appropriate encryption applied. By their nature mobile devices are easily moved and devices can potentially carry very large amounts of personal data. Policy relating to this can be found in **METSEC Code TEC9.3 Encryption for Mobile Devices & Media**; the **Mobile Computing SOPs** and the **Working Away from the Office (WAFTO) SOPs,** which are mandatory upon all MPS personnel. Paper documents and photographic media etc. containing personal or protectively marked data taken off MPS premises are to be carried under cover and not left unattended. For further details see **METSEC Code PER5 - the Protection of Unattended Information**. The information security documents referred to can be found at the following link: Information Management & Security Policy & Procedures.

The requirements can be complex in an organisation on the scale of the MPS. It may cover areas including information technology security, physical security, vetting processes and the application of protective marking of data, etc. Further advice and guidance on information security issues referral must be directed to the Information Assurance Unit DoI2 (3-1).

15.0 PRINCIPLE 8 – NOT TRANSFERRED TO OTHER COUNTRIES WITHOUT ADEQUATE PROTECTION

The requirements and provisions of Principle 8 are detailed in the International Data Processing SOPs

16.0 EXEMPTIONS

The Data Protection Act 1998 provides a number of exemptions from aspects of the Act. These particularly concern certain basic aspects of the Act such as restrictions on providing personal data to third parties, and the right of access by data subjects to their personal data which are considered and applied by the PAO. There are very few exemptions from the entirety of the Act, although there are some exemptions from much of the Act.

Exemptions under the Act can appear complex and need to be considered on a case by case basis. Where an exemption is to be considered outside 'normal business processes' or areas are detailed within this SOPs this should be discussed with the

Data Protection Officer. Below are detailed brief descriptions and applications of the exemptions available concentrating on those most relevant to the MPS:

- **Crime and Taxation (Section 29)** - This exemption has two main uses within the MPS. The exemption provides a legal gateway for other bodies to provide information to the MPS without breaching DPA rights and requirements.

  A request for information from another organisation can be made on **form 3022 (Data Protection - Personal Data Request Form)** available via the forms unit MPS Corporate Forms Index.

- The second main use of this exemption is in regard to subject access requests made by individuals when the disclosure of information requested is likely to prejudice the prevention and detection of crime. This exemption can be used to refuse or redact a disclosure in these circumstances;

- **Disclosures required by law or made in connection with legal proceeding (Section 35)** - Provides the MPS with the opportunity to release information to individuals and their representatives where legal action is ongoing or considered. This exemption provides the avenue for a Data Controller to provide such information. However, it does not compel or provide an obligation that information must be provided. Releases can only be required in the case of disclosures required by law or via a court order for disclosure. Further information regarding the handling of requests for information related to legal proceedings and Section 35 are detailed in Section 17, 'Requests for Information Regarding Legal Proceedings'.

- **Regulatory Activity (Section 31)** - Provides an exemption around the processing of a subject access request. This exemption can be used by the PAO when dealing with a request involving information which may prejudice an investigation by the Independent Police Complaints Commission or other regulator upon disclosure. This exemption may be considered in regard to an ongoing Directorate of Professional Standards (DPS) investigation, however as a Section 29 exemption may also be available that would always be relied upon in the first instance;

- **Legal Professional Privilege (Sch 7 Para 10) -** Personal data is exempt from disclosure where there is a claim of legal professional privilege between the MPS and our legal advisors on a client basis. This will include advice sought from the DLS, MPS instructed solicitors and outside counsel.

- **National Security (Section 28)** - The national security exemption provides an exemption from a number of areas and provisions of the DPA. The exemption allows for the obtaining, holding and processing of national security related information

without the full requirements of the Act. The exemption is utilised only in exceptional circumstances due to the ability to engage the Section 29 exemption. Where the Section 28 exemption is considered for large scale projects with partners the Data Protection Officer will need to be consulted. There is a requirement under the Act that a certificate signed by a Minister of the Crown is required to demonstrate appropriate application of the exemption where required. An example of the use of the Section 28 exemption is in an agreement with Transport for London (TfL) in the access to Automatic Number Plate Recognition (ANPR) data for national security purposes, which is then supported by a Ministerial Certificate;

- **Health, Education and Social Work (Section 30)** - Provides the Secretary of State with the power to make an order in relation to information held on the physical or mental health or condition of a data subject. The publication of the *Data Protection (Subject Access Modification) (Health) Order 2000* instigated these powers which allows an appropriate medical professional to exempt information from release under subject access where it is likely to cause serious harm to the physical or mental health of the subject. The MPS is not able to apply this exemption in isolation but only on the written approval of the medical professional responsible for the clinical care of the data subject. This exemption is likely to have limited application and most likely in scenarios or areas where the release of MPS information is likely to seriously affect the mental health of the data subject, namely information held in areas such as the Fixated Threat Assessment Centre;

- **Research, History and Statistics (Section 33)** - Where personal data is used for solely research, history or statistical purposes it is exempt from a number of provisions of the Act. This is unlikely to affect the majority of MPS data as it may be used for statistical purposes but will initially be held for an additional purpose i.e. investigation or HR matters;

- **Confidential References (Schedule 7 Para 1)** - Employment references supplied by the MPS to employers regarding an existing or previous MPS employee can be withheld from disclosure to the data subject under this exemption. This exemption does not extend to requests to access copies of employment references supplied to the MPS during the course of our recruitment processes; however, there may be a duty of confidence owed to the referee, which we must consider before disclosure is made under the Subject Access Provisions.

- **Management Forecasts (Schedule 7 Para 5)** - Provides an exemption to the release of information under subject access where personal data is being used for

management forecasting or planning where that release would prejudice the work of the MPS;

- **Negotiations with the Data Subject (Schedule 7 Para 7)** - Similar to the above, this is an exemption where disclosure is exempt on negotiations with the data subject if the release would be likely to prejudice those negotiations;
- **Examination Marks (Schedule 7 Para 8) & Examination Scripts (Schedule 7 Para 9)** - Provides exemption from subject access in relation to personal data contained in examination scripts and the access to examination marks which are normally published; and
- **Self Incrimination (Schedule 7 Para 11)** - Information is exempt from disclosure under subject access where that information would incriminate the MPS in the commission of an offence, other than those offences found under this Act (see section 19).

17. INFORMATION SHARING & DISCLOSURE

Detailed advice on sharing personal data with third parties is contained within the Information Sharing SOPs:

Information Sharing with Partner Organisations SOPs

The MPS receives regular requests to access the personal data we hold from a wide variety of requesters for a variety of purposes. Each request must be considered on a case-by-case basis to ensure that legally the information can be shared and that the sharing is physically carried out using a secure method.

Where it is not clear whether there is a lawful basis for the request advice should be sought from the Information Sharing Support Unit (ISSU), DoI2 (3-3) Public Access Office (PAO). Advice provided in the SOPs and by the ISSU covers both ad-hoc information sharing and the processes and procedures in setting up formalised information sharing through the production of information sharing agreements (ISAs)/other protocols.

Requests for information regarding legal proceedings

- **Requests for limited particulars to instigate legal proceedings** - It is common place for the MPS to be contacted by victims or their legal representatives to request the contact details of those who committed crimes that has resulted in damage/ distress to the victim which could be compensated for via the civil litigation process. If

an individual has suffered loss or injury because of the activities of another individual, they may have a legal right to sue for compensation.

Where an allegation has been made to the police, the aggrieved party may request the name and address of the other party, in order to consider taking legal action. Section 35 of the DPA states that personal data is exempt from non-disclosure for the purpose of obtaining legal advice, or defending legal rights and so on. **Please note -This exemption is dependent on the officer in charge (inspector or above) being satisfied that a sufficient risk assessment has been actioned and satisfied.** A risk assessment should be carried out to ascertain whether there is any information indicating potential harm to the suspect if his or her details are disclosed. In the absence of such information disclosure can take place if the officer, inspector or above, is satisfied that the information requested is required to instigate legal proceedings and the public interest in the victim being able to pursue a claim for compensation outweighs the suspects right of confidentiality. There is no legal restriction on the disclosure of a juvenile's details, though clearly the age of the suspect will be one of the matters considered in the risk assessment. The outcome of the risk assessment and confirmation of any disclosure should be documented either on the associated Crime Recording Information System (CRIS) record if held or stored in the Criminal Justice Unit on Borough Operational Command Unit and retained as per the MPS Retention Schedules.

- **Requests for further information** - Additional to the requests for base level data the MPS will receive requests from solicitors in regard to ongoing or intended legal proceedings often requesting substantial amounts of information. Where the MPS is party to the intended or current proceedings these requests should either be passed to, or completed, in association with the Directorate of Legal Services (DLS).

  Where the MPS is not party to the action the request should be considered on a local level whether the MPS wish to provide disclosure proactively. Section 35 allows the disclosure of information but this is not an obligation so the decision can be made to refuse a request. If a request is refused a solicitor will be in a position to approach the courts to seek a court order for disclosure of the relevant information. Therefore any decision to release information **must** always be recorded including a summary of what information was disclosed, the date and to whom as per the recording process above.

- **Requests for information from Insurance Companies and Loss Adjustors -** Insurance Companies have a process to access the personal data of their clients following an insurance claim similar to the subject access process. This process is enshrined in the Association of Chief Police Officers (ACPO) and Association of British

Insurers Memorandum of Understanding (ABI MoU) which provides guidelines on the exchange of information between the Police, insurance companies and loss adjustors. All requests relating to individual data subjects are dealt with by the PAO as detailed at the following link.

Data Protection - advice regarding insurance companies & loss adjusters

Any requests for information related to individuals from insurers and loss adjusters must be forwarded to the PAO with 48 hours of receipt - If requests are received related to corporate loss (excluding sole-traders, which the PAO will be able to process) or insurance companies without ABI member association these will be returned to the investigating borough to consider disclosure. As per legal proceedings there is no obligation in these circumstances to provide information, however a consideration should be made of the benefits of disclosure.

Notifiable Occupation Scheme - Provides a route for the MPS to update employers for certain occupations when an individual comes to police notice or is charged for an offence. The SOP is linked below:

Notifiable Occupation Scheme SOPs

Family Proceedings - Provides information to parties involved in family proceedings. The following SOPs details the process in relation to private law firms and the Children and Family Court Advisory and Support Service (CAFCASS) when making requests for information in support of family proceedings. This process is currently managed by SCD5 Child Abuse Investigation Command with assistance from the Directorate of Legal Services (DLS).

Protocols on Sharing Information in Family Proceedings SOPs

Researchers - Requests for personal information from researchers should be discussed with the Strategic Research and Analysis Unit within Directorate of Resources (DoR).

MPS Strategy & Improvement Department Research Advice

Requests from Family Members of Deceased Individuals - Where families are requesting information regarding deceased relatives' consideration should be made in regard to the processing of that request. As the Data Protection Act 1998 (DPA) only applies to data of living individuals it does not automatically cover the 'rights' of any deceased individual, i.e. there is no subject access right available that can be used by their surviving family members. Requests may be received in the form of a Freedom of Information Act 2000 (FoIA) request.

However again this may not be seen to be suitable legislation to meet the request as there may be an outstanding duty of confidence to the deceased individual or the release of information may breach the DPA or HRA rights of a third party.

The MPS will discuss such cases with the family concerned in order to review the information required and assess whether information can be provided outside of these acts as 'normal business'.

- Where information is requested regarding the conviction history of a deceased individual this will be reviewed by the SCD12 Information Management Team;
- Information in relation to specific incidents and the deceased individuals' involvement should be reviewed by the investigating Borough or OCU; and
- If the information requested relates to the service history or other employment data of a deceased former member of the MPS this should be referred to the MPS Historical Collection or Records Management Branch.

Media Requests - Requests for personal information from the media are detailed in the guidance provided by the Directorate of Public Affairs in the SOP linked below:

Media Relations SOPs

18. DATA COLLECTION

18.1 The Overt Collation of Personal Data

There are a number of ways in which the MPS collates personal information overtly through day to day policing activities such as stop and searches, arrests and the taking of witness statements. The collection of this information must be both Fair and Lawful in accordance with the DPA Principles and as detailed within the MPS Fair Processing Notice.

18.2 The Covert Collation of Personal Data

The covert collection of personal data is covered by the Regulation of Investigatory Powers Act 2000 (RIPA). Advice on specific cases should always be sought from the relevant authority within the MPS, SCD10 Covert Policing Command or from the PAO if general information or advice is required.

RIPA: UK Legislation - RIPA

SCD10: MPS Covert Policing Command

19. CRIMINAL OFFENCES

The Commissioner of Police of the Metropolis is ultimately responsible as data controller for the acts and omissions of his personnel and agents and the office of Commissioner of Police can be prosecuted under the DPA due to this vicarious liability. The MPS Commissioner can also be fined under the statutory powers granted to the ICO and such fines can be heavy (up to £1/2 million per offence).

It must also be appreciated that individuals processing data on the data controller's behalf can themselves be liable individually for prosecution under the Act in certain circumstances.

Furthermore, MPS personnel who misuse or are otherwise negligent in their handling of personal data can be liable for disciplinary action under the appropriate codes of conduct. Unauthorised disclosure of personal or sensitive personal data is strictly forbidden and will be considered as gross misconduct. It should be understood that in serious cases dismissal from the Service will be an option to be considered. The following is a list of some of the criminal sanctions under the Act but it is not exhaustive:

- **Sections 17 to 21** – Covers non-notification offences to the ICO. This offence is linked to the requirements on the Data Controller and the Data Protection Officers notification of the ICO;
- **Section 47** – failure to comply with an enforcement notice, information notice or special information notice issued by the ICO;
- **Section 55** – unlawful obtaining, disclosing or procuring of personal data and the selling (or offering for sale) of personal data unlawfully obtained, disclosed or procured. **Within the Police Service Section 55 is the most relevant offence under the Act as it appertains to members of the MPS unlawfully obtaining or disclosing data from MPS systems**;
- **Schedule 9, paragraph 12** – intentional obstruction of, or failure to give reasonable assistance in, the execution of a warrant sought by the ICO;
- **Section 56 (not yet in force)** – enforced subject access offence. Once enacted this offence will be relevant to employers or other bodies that force individuals into making subject access requests of a particular reason. For example, where employers not subject to the Criminal Records Bureau (CRB) request an applicant provide a Police National Computer (PNC) subject access request disclosure as a prerequisite to employment.

Assistance with the preparation of these offences should be sought from the PAO in liaison with the DPS or the CPS as required.

20.0 REQUEST FOR DISPENSATION TO USE PERSONAL DATA FOR TEST OR DEVELOPMENT PURPOSES

The DPA states that personal data may only be used for the specified lawful purposes as defined within the 'MPS Fair Processing Statement' and the 'Registered Purposes'. Therefore, personal data **must not** be used for test or development purposes without the authority of the Data Controller (the MPS Commissioner). The Data Controller will consider each case on its merits. Only exceptional situations when there is a compelling case will approval be given this approval requires the submission of the **corporate form 3018** see MPS Corporate Forms Index to the Data Protection Officer (DPO) or their Deputy (DDPO). See also **METSEC Code EAA2.6.4 Use of Personal Data for testing or development is usually prohibited**.

21.0 DATA PROCESSING AGREEMENTS

The MPS frequently uses outside organisations to process its Data and this can be due to contractual or other reasons. It is important that where data processing is being completed on behalf of the MPS it is done strictly in accordance with the requirements of the DPA. In order to formalise this process the DPA requirements should make up part of the contractual arrangements or be subject to a separate data processing agreement. This must formalise the requirements the MPS sets for that organisation and any provision for penalties if these requirements are not met. Further advice on this area can be sought from the Data Protection Officer (DPO).

A template data processing agreement can be found in the Association of Chief Police Officer's DPA Manual of Guidance available at:

ACPO Data Protection Manual of Guidance

22.0 RESPONSIBILITIES

Ownership of SOPs: Enterprise Architecture Board (EAB) (Directorate of Information)

Implementing SOPs: DoI2 (3-3) Public Access Office (PAO)

Compliance with SOPs: DoI2 (3-3) Public Access Office (PAO)

23.0 ASSOCIATED DOCUMENTS & POLICIES

23.1 Associated & Linked Reference Documents

- Information Management Policy
- Information Sharing with Partner Organisations Standard Operating Procedures (SOPs) v5.0
- Compliance Standard for International Data Processing Standard Operating Procedures (SOPs) v1.0
- Mobile Computing Security SOPs v2.0

Evidential Images SOP

Evidential Images SOPs

MPS Use of Custody CCTV

Custody Policy & SOPs

23.2 Relevant Forms

- Form 696 - Promotion Event Risk Assessment Form
- Form 1000 - Request to department of Work &Pensions for information under S.29(3) DPA 1998
- Form 3018 - Request for Dispensation to use Personal Data for Test or Development Purposes
- Form 3019 - Application for access to your Personal Data held on the PNC or MPS Information Systems (also known as the Subject Access Request form)
- Form 3022 - Request for Personal data from outside organisations

23.3 Relevant Legislation

- Data Protection Act 1998 (DPA)
- European Data Protection Directive 95/46/EC
- Statutory Instrument (SI417/2000) - Processing of Sensitive Personal Data
- Freedom of Information Act 2000 (FoIA)

- Human Rights Act 1998 (HRA)
- Crime & Disorder Act 1998
- Criminal Justice & Police Act 2001
- Police & Criminal Evidence Act 1984
- Equalities Act 2010 (EA)

23.4 Documents Replaced

- MPS Security Policy Manual (METSEC Code) - Section LGL1 Data Protection Act 1998
- Data Protection - Subject Access Standard Operating Procedures (SOPs) v3.2
- Data Protection - Obtaining Personal Data from Outside Organisations SOPs v2.2

23.5 Notices to be cancelled

Additional to section 23.4 the following documents are cancelled and withdrawn:

- Item 3, Notices 05-2007 Disclosure of suspect's details to victims of crime

24.0 ABBREVIATIONS & DEFINITIONS

24.1 Abbreviations

ABI MoU	Association of British Insurers Memorandum of Understanding
ANPR	Automatic Number Plate Recognition
ACPO	Association of Chief Police Officers
CAFCASS	Children & Family Court Advisory & Support Service
CCTV	Closed Circuit Television
CRB	Criminal Records Bureau
CRIMINT	Criminal Intelligence System
CRIS	Crime Recording Information System
DD&D	Damage, Damage and Distress
DPA	Data Protection Act 1998
DPO	Data Protection Officer
DDPO	Deputy Data Protection Officer
DLS	Directorate of Legal Services
DPS	Directorate of Professional Standards
DWP	Department of Work & Pensions
EA	Equalities Act 2010
EEA	European Economic Area
EU	European Union
FoIA	Freedom of Information Act 2000
HR	Human Resources
HRA	Human Rights Act 1998
IAU	Information Assurance Unit

ICO	Information Commissioner's Office
IGF	Information Governance Framework
IPF	Information Policy Framework
ISA	Information Sharing Agreement
ISSU	Information Sharing Support Unit
MoPI	Management of Policing Information
MAPPA	Multi-Agency Public Protection Agreements
MPA	Metropolitan Police Authority
MPS	Metropolitan Police Service
OCU	Operational Command Unit
OH	Occupational Health
OIC	Officer in the Case
PACE	Police & Criminal Evidence Act 1984
PAO	Public Access Office
PIA	Privacy Impact Assessment
PNC/ PND	Police National Computer/ Database
RIPA	Regulation of Investigatory Powers Act 2000
RMB	Records Management Branch
SARs	Subject Access Requests
SI	Statutory Instrument
SyOps	Security Operating Procedures
SOPs	Standard Operating Procedures
TfL	Transport for London
VRM	Vehicle Registration Mark

25. CONTACTS & SUGGESTED AMENDMENTS

25.1 Contacts

Data Protection Officer (DPO)

Deputy Data Protection Officer (DDPO)

Information Security Officer (ISO)

25.2 Amendments

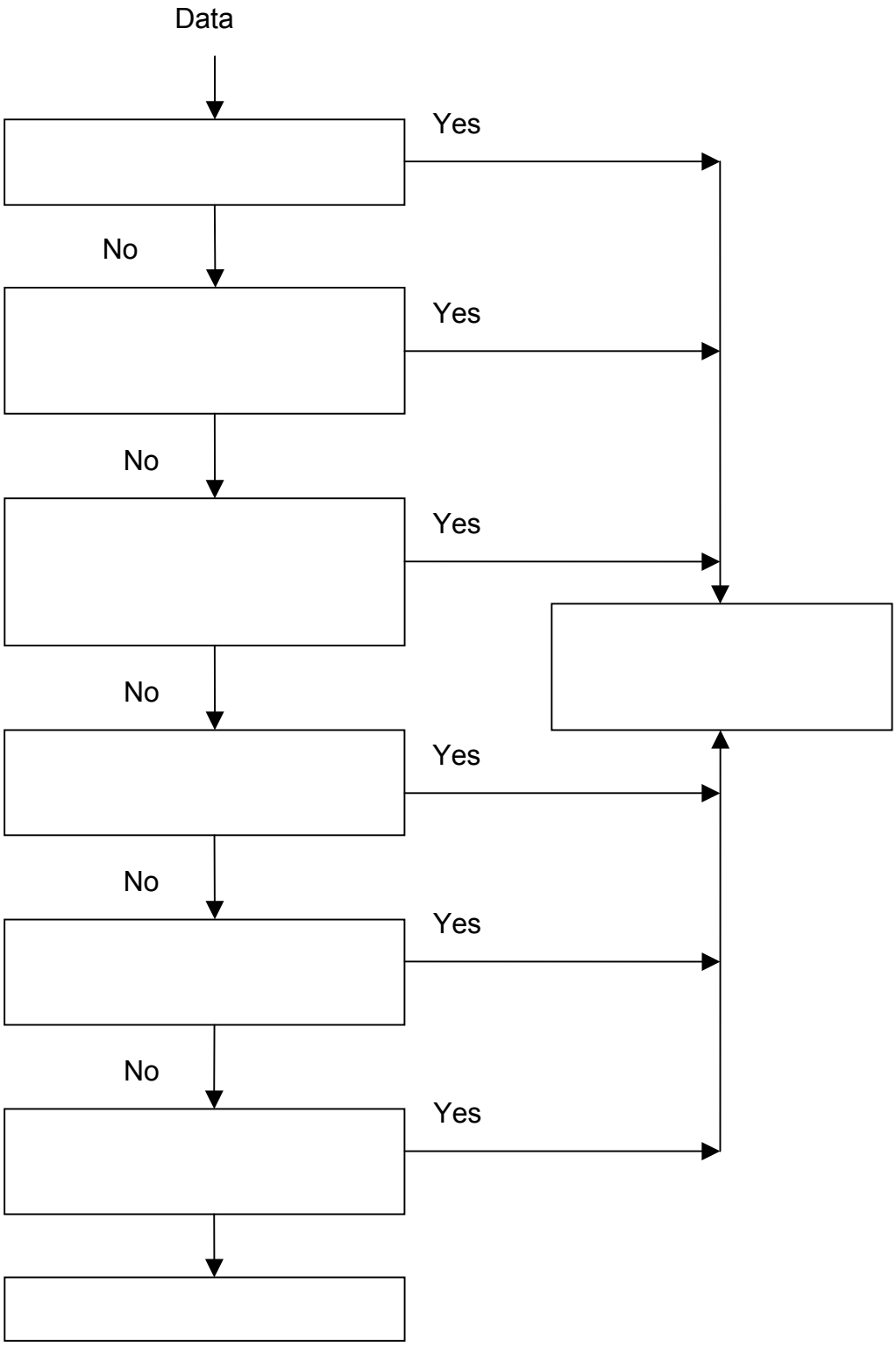
Any suggested amendments to inform future SOPs, or highlighting any spelling or grammatical errors within this document can be communicated either using the corporate policy Feedback Form found on the Corporate Policy Database; by email to 'DoI Mailbox - Security Advice' or in writing via despatch to Information Assurance Unit (IAU), DoI2 (3-1), Floor 1 West, Edinburgh House. Any suggestions will be noted for consideration to change the SOPs as deemed appropriate at the next review.

APPENDIX A - DPA QUICK REFERENCE GUIDE

The purpose	• The Act is designed to regulate the processing of personal information and ensure its protection in line with the rights afforded to individuals under Article 8 of the Human Rights Act 1998 and EC Directive 95/46/EC.
The basics	• The Act refers to all personal data in relation to identifiable living individuals. • The Act has 8 Principles which underpin the requirements which need to be met in order to process personal data lawfully. • The Act also gives an individual the right to request a copy of any information held about them by the Police Service, subject to the application of relevant exemptions. • The right of access applies regardless of the purpose of the application. • The Act also provides rights to individuals to prevent data processing which is likely to cause damage/ damage and distress (DD&D), claim compensation for DD&D and seek the rectification/ destruction of inaccurate information. • The Act also makes certain personal data processing a criminal offence, including (but not limited to) unlawful obtaining or disclosure of personal information, and the processing of personal data without registration with the Information Commissioner (ICO).
Validity of requests to access personal data	To be valid under the Data Protection Act 1998, requests: • Must be made in writing (using the 3019 form); • Provide sufficient identification • Include a £10 fee (made payable to the Metropolitan Police Authority); • Must clearly describe the information being sought in order to locate the information; • Can be made by the individual or his/ her representative as long as the representative has written authority from the data subject that they can act on their behalf. • To be valid under the Data Protection Act 1998, requests do not need to refer to the 'Data Protection Act' (DPA) in any way.
What is covered?	The Data Protection Act 1998: • Covers all records, data and files containing personal information capable of recovery in any form. • Is fully retrospective: as long as the MPS holds the personal information it is covered by the requirements of the DPA, this includes MPS information processed or held by any member of the MPS at their home or any other non-MPS address (this would include personal computers/ email). Such data handling would be subject to security risk implications, but additionally would make the IT used to process that information subject to MPS DPA processes including the right of access to information. • This includes (some) research reports, pocket note books, written records, typed, handwritten, e-mails, CCTV, audio

	tapes, computer tapes, system entries/ logs, answer phone messages, tapes of telephone conversations, photos, fingerprints, DNA, post it notes and archived records. • The Act includes all methods of processing including obtaining, recording, holding, organisation, adaptation, alteration, retrieval, consultation, alignment, combination, blocking, erasure, destruction, disclosure, transmission, dissemination, or otherwise making available the data or information.

APPENDIX B - Flow Chart Diagram - Is it Personal Data?



Appendix C - Fair Processing Template for Forms Used by the MPS to Collate Personal Data

- Provide the identity of the organisation in control of the processing;
- Provide the purpose, or purposes, for which the information will be processed; and
- Any further information necessary, in the specific circumstances, to enable the processing in respect of the individual to be fair.

In some cases individuals are required by law to provide their personal details. Where this is the case, seeking consent is not required and is often of no value. Instead, organisations should be open with people and explain clearly why their information is being collected and what it will be used for. Even if individuals have no real choice, the collection of information about them still has to be fair and transparent and a privacy notice can be used to make sure that this is the case.

For further information on how your information is used, how we maintain the security of your information, and your rights to access information we hold on you, please contact: (clear web link/ free phone etc.).

Specific Policing Purpose/ Need for the MPS requiring the Data e.g. The Promotion Event Risk Assessment Form 696 is designed to allow the management of licensed premises, promoters of music events, event security and the police to work in partnership to identify and minimise any risk of serious violent crime happening at a proposed event. Should areas of concern be identified the police intention is to work together to create a Risk Management Plan that enables the event to proceed with minimum risk.

Is the Data collation Voluntary or Compulsory? e.g. The use of this form is voluntary. However, we note that the completion of this form may be a condition on some premises' licences. This means the completion of this form is mandatory for those premises. The management of the licensed premises or the promoter considers that the proposed event requires a Promotion Event Risk Assessment Form 696 to be completed and it is for this purpose that your personal details are required

What will the MPS do with the Information and how long will the MPS retain the Information For? e.g. The information provided will be cross-referenced with our systems and data sources to assist with the risk assessment. The information will be retained on our systems for 2 years at which point it will be reviewed for deletion or, if there is a specified policing purpose to retain the information for a further defined period.

Information collated and processed for a Policing Purpose must be in line with our Policing Purposes and the Data collation either Voluntary or Compulsory? e.g. - The information is processed in accordance with our policing purposes as defined by the Code of Practice for the Management of Police Information (MoPI) as follows:

• Protecting life and property;
• Preserving order;
• Preventing the commission of offences;
• Bringing offenders to justice; and
• Any duty or responsibility arising from common or statute law.

If you or your client has any concerns or queries regarding the above processing please contact the Metropolitan Police Service Data Protection Officer (details provided below):

- **Data Controller Details:** Sir Paul Stephenson, the Commissioner of Police of the Metropolis (**Information Commissioner's Office Data Controller Registration Number:** Z4888193)

- **Data Protection Officer Details:** Merilyne Knox, Public Access Office, and PO Box 57192, London, SW6 1SF (Tel: 020 7161 3500)

For a copy of the Metropolitan Police Service's Fair Processing Notice please refer to the following link or contact the Data Protection Officer (details above):

MPS Fair Processing Notice:

http://www.met.police.uk/foi/pdfs/other_information/corporate/mps_fair_processing_notice.pdf