



**METROPOLITAN
POLICE**

Freedom of Information Act Publication Scheme	
Protective Marking	Official
Publication Scheme Y/N	Yes
Title	Met Data and Technology Management Policy
Version	1.0
Summary	This Policy provides a framework for the management and control of Met data and technology assets, in all formats
(B)OCU or Unit, Directorate	Met HQ Strategy and Governance – Information Law & Security - Information Assurance Unit (IAU) and Digital Policing
Author	Information Policy Developer, Information Assurance Unit (IAU) Met HQ
Review Date	December 2023
Date Issued	December 2019

Freedom of Information Publication Scheme					
GSC	OFFICIAL			Publication (Y/N):	Y
Title:	Met Data and Technology Management Policy				
Summary:	This Policy provides a framework for the management and control of Met data and technology assets, in all formats.				
Branch / OCU:	Met HQ Strategy and Governance – Information Law & Security - Information Assurance Unit (IAU) and Digital Policing				
Date created:	2 nd December 2019	Review date:	December 2023	Version:	1.0
Author:	Information Policy Developer, Information Assurance Unit (IAU) Met HQ				

MET DATA AND TECHNOLOGY MANAGEMENT POLICY

Policy Application

- **When?** The **Met Data and Technology Management Policy** applies with immediate effect. It now combines and updates the previous **Information Management (IM) in the MPS Policy** with the **Management and Use of Technology Assets Policy**, first issued 17 March 2010.
- **Who?** All police officers and police staff, including the extended police family and those working voluntarily or under contract to the Mayor's Office for Policing and Crime (MOPAC) or the Commissioner must be aware of, and are required to comply with, all relevant Metropolitan Police Service [MPS or Met] policy and associated procedures.

This Policy applies to all Met personnel [both managerial and non-managerial roles] dealing with data [*aka as information*] and technology in both a professional and private capacity. It places an expectation of trust on individuals to handle **Met data** and the **technology assets** that process that information, appropriately and with due care and diligence in accordance with the policy, procedures and guidance.

The following roles have a particular responsibility to ensure that personnel under their control and direction are fully briefed and aware of Met Data and Technology Management Policy requirements [*This list is not exhaustive*]:

- Basic Command Unit (BCU) Commanders; Heads of Directorates or Branches
- All line managers and supervisors
- Information Asset Owners (IAOs), BCU security champions and local decision makers

What?

This policy relates to the management, security and control of **Met Data Assets**. Met data is to be security classified, utilised and protected according to its intrinsic value connected to specific policing requirements, such as criminal records or intelligence purposes. It includes the data itself and the use of information communications and technology (ICT) systems and processes that deal with such data across all policing and support activity.

Met Technology Assets will at all times be managed and used in such a way as to gain maximum operational and business benefit from the technology while maintaining an adequate and appropriate asset management, systems administration and security regime. To achieve this end, all officers, staff and contractors using or involved in the management of these assets and their data will:

- Comply with relevant legislation as detailed in any Standard or Security Operating Procedure.
- Comply with relevant Codes of Conduct or Practice, other documents or notifications governing the use of the technology and its associated standards detailed in any Standard or Security Operating Procedure.
- Comply with all other aspects of the Standard or Security Operating Procedures listed within this policy document or controls framework; such as [but not limited to] the allocation, issue, use, maintenance and care, data and device security, storage on and return of the technology assets.

Definition of Met data/ information - In this context, the word 'information' equates to and has the same meaning as 'data'. The terms are largely interchangeable, but data tends to be preferred with reference to any information held in an electronic rather than a paper form. In addition, the term 'Met or MPS information' includes all information collected, created and received by the Met that is used in relation to any operational policing or organisational support function. It will occasionally include data originally collected by other police forces and crime agencies held in common on national policing systems. The specific term 'police information' is in effect operational information required for 'policing purposes', further defined in the **Management of Police Information (MoPI)** section in the **Data Governance Framework (DGF)**.

Data formats - It should be noted that Met data/ information exists in many different formats to support business need. It includes paper documents ['hard copies']; electronically held computer

and communications information [i.e. electronic digital/ 'soft copy' data]; or other technological means, such as that recording photographic/ audio/ video media [i.e. CCTV, radios and Body Worn Video (BWV)].

Policy Purpose and Benefits

The **Met Data and Technology Management Policy** supports the Data Strategies and Corporate Strategy, including the One Met Model 2025 vision to make London the safest global city in the World. The application of good data management practice combined with modern ICT helps achieve making London and its communities safer. The vision is to create a data-driven organisation, where policing actions are timely and fully informed. To further this aim, the policy design supports the application and compliance with any technical, professional standards and all relevant legal requirements. The latter for example includes personal data processing in accordance with the **Data Protection Act 2018 (DPA)** and the **General Data Protection Regulation (GDPR)** requirements. To achieve these objectives, the policy and supporting procedures/ standards provide instructions/ guidance to all personnel for the proper management and control of Met data and the supporting technology assets that holds such data.

The **Met Data and Technology Management Policy** will therefore enable the Met to provide trusted and valued data when required for policing purposes at the point of need through:

- Security assurance aligned to modern ICT infrastructure, systems, applications and services, including use of mobile devices and a range of media
- Legal and secure procedures for the processing of Met data
- Standards of control and accountability over data use and ICT systems administration
- The application of data quality standards and analysis/ profiling of data to improve policing outcomes in the public interest
- Providing information access services to the public
- Appropriate and lawful sharing of data with trusted partners
- The safe disposal of recorded information when no longer required and

- Demonstrating and evidencing to policing and other authorities, our partners and the public that we remain an organisation fit to be trusted with holding and using data appropriately [i.e. legally/ ethically]

Policy Principles

- The Met Data and Technology Management Policy supports our Data Strategies, the Corporate Strategy and Policing Plan.
- The Met will manage data to ensure that, subject to appropriate security and legal requirements, it is readily available to all those who need to use it in their police work.
- The Met will manage data to ensure that subject to appropriate security and legal considerations the data provided to the public, is in formats that are accessible, accurate and easy to understand.
- Procedures, standards or toolkits will exist to provide effective, efficient and legally compliant procedures and guidance for the processing of all Met data assets. The term 'processing' includes the collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.
- The Met will promote measures highlighted in procedural documentation to ensure that all users of Met data and ICT systems are aware of their data management responsibilities, including that relating to the ICT technology assets that supports it. These measures include, for example, completion of mandatory or specific training courses to provide a high degree of compliance/ assurance that data processing is both legal and appropriate.
- All Met staff and others who process Met data [including those who create, use, manage, protect, exploit (e.g. share, disclose, analyse) or dispose of] **must** do so in accordance with the law, procedures/ toolkits and other documentation provided.

The Met Data and Technology Management Policy supports a number of procedural documents covering the following components, which implement the said policy in practice. These documents can cover and link to other similar procedures [*including other corporate or national police policy*], inter-related disciplines, or involve work across business units, as follows:

- **Met information security procedures** [e.g. the Government Security Classification (GSC)];

- **Other information assurance requirements** and the application of the **Digital Policing - Controls Framework** and other technical measures for management of the Met ICT infrastructure, systems [*development and in service administration*], applications, equipment and services;
- **Management of Police Information (MoPI)** requirements [*also see Authorised Professional Practice (APP)*]
- **Records Management (RM) Policy** compliance [*which now includes MoPI/ National Policing RM Policy requirements*];
- **Data quality and insight** [*e.g. compliance with Home Office crime recording standards*];
- Compliance with **Information Rights Law** [*Data protection, freedom of information and other statutes/ case law*]; and
- **Data sharing** as agreed with trusted partners [*see the Share Met Information Policy for further details*].

Note: This list is not exhaustive.

Associated Documents and Policies

Support for this document [the **Met Data and Technology Management Policy**] comes from the following loaded or listed standard operating procedures (SOPs), data toolkits and guidance:

Many of the said procedures and guidance are found in a series of documents posted internally on the Intranet under 'Support - Information Management' at - <http://mpsweb.intranet.mps/support/information-management/>

Strategies

3x Data Strategy [Data Strategy; Analytics Strategy and Talent Management Strategy] documents to be linked from here.

Policy enablers [*links to DGF documents loaded into Useful Resources*]:

Data Governance Framework (DGF) v1.0 05Nov2019

Appendix A - Data Governance Framework (DGF) Table 05Nov2019 v1.0

[The METSEC Code \[The Met's Security Manual\]](#)

[MPS Information Code of Conduct](#) [also on the Foundation desktop under 'InfoSec documents']

Security:

[Government Security Classification \(GSC\) policy](#)

[Use of Met Computer Systems Policy](#)

[Report a security incident or data breach](#)

Legislative:

[Data Protection Act 2018 \(DPA\) Compliance Policy and Guidance](#)

[Share Met Information policy](#)

[General Data Protection Regulation \(GDPR\) Fact Sheet 1](#)

[Freedom of Information Act 2000 \(FoIA\) Policy](#)

Information & Records Management:

[Records Management \(RM\) Compliance Policy and guidance](#)

ICT Assets:

[AIRWAVE Standard Operating Procedures \(SOP\)](#) [pending update]

[Met Supplied Smart Phones Guidance](#)

Foundation User Security Operating Procedures (SyOps) – Located on the AWARE desktop under 'I for Infosec Docs.

Other MPS documents:

Forms - [Forms - New Database](#)

Form 3018 - Request for Dispensation to Use Personal Data for Test or Development Purposes

Form 3022 - Personal Data Request [from other organisations]

Useful 'Data Office' [Met HQ Strategy & Governance - Information & Insight] Intranet contact pages:

[Information Assurance Unit](#)

[Information Rights Unit \(IRU\) Homepage](#)

[Records Management Team \(RMT\) Homepage](#)

[Met Data Insight Hub](#)

[Met Performance Pages](#)

[SNT Analytics](#)

[Data Accuracy Team \(DAT\)](#)

External web resources

[Information Commissioner's Office \(ICO\)](#)

[Police National Legal Database \(PNLD\)](#)

[College of Policing Authorised Professional Practice \(APP\) - Information Management](#)

[HMG Legislation database](#)

[The National Cyber Security Centre \(NCSC\)](#)

[The Centre for the Protection of the National Infrastructure \(CPNI\)](#)

Associated Met Policies

The data/ ICT management and security elements described by this policy is applied in combination with the unit details and documents listed below. This is to provide a more comprehensive set of instructions for MPS security across all assets, i.e. people, property and as well as data:

- [Digital Policing](#) are responsible for the provision of the main ICT equipment and services in the Met. Please note that the former Management and Use of Technology Assets Policy is now incorporated into this policy. This enables the further issue of procedural and guidance documents to match technological change and introduction of new data services.
- [Met Vetting Unit](#) and Corporate ID Documents [[Issue of warrant cards & staff passes](#) and non-police personnel passes], issuing and their management requirements.
- Risk Management Policy [incorporates Business [Risk Management](#) and [Business Continuity Policy](#)]; and
- [Security of the Met Estate Policy](#) and [Counter-Terrorism Safety Advice](#)

National policies and guidance:

- [College of Policing Authorised Professional Practice \(APP\) - Information Management](#)
[Includes APP Guidance on the Management of Police Information (MoPI)]
- National Policing Information Systems Community Security Policy (CSP)
- National Policing Accreditation Policy for National Police Systems
- National Policing Governance and Information Risk Return (GIRR)
- The **National Police Chiefs' Council (NPCC) Guidance on The Minimum Standards for the Retention and Disposal of Police Records**
- HMG Security Policy Framework (SPF) and the data security standards, notices and guidance issued by the following governmental agencies - [The National Cyber Security Centre \(NCSC\)](#) and [The Centre for the Protection of the National Infrastructure \(CPNI\)](#)

Notices to cancel/ amend and Policy documents to be de-commissioned

Cancel – Item 6, Notices 12/ 10 of 17 March 2010 [**Use and Management of the Technology Assets Policy**]

De-commission - Information Considerations when Repairing, Re-using or Disposing of ICT Equipment & ICT Storage Media Standard Operating Procedures, v3.0 dated 7 March 2011

All enquiries and feedback for this policy statement – Direct to the Information Policy Developer, Met HQ - Information Assurance Unit, on internal extension **785327** or e-mail to 'IAU Mailbox - Security Advice'.

Report all ICT/ telephony faults or needs via the Intranet online IT Portal or on telephone x69555.

Equality Impact Assessment (EIA)

All Public Authorities, including the Met, have to comply with **section 149 Equality Act 2010**. This provision is more commonly known as the general public sector equality duty.

This general equality duty requires us to:

- Eliminate discrimination, harassment and victimisation plus other conduct prohibited by or under the Act.
- Advance equality of opportunity between people who share a relevant protected characteristic and people who do not share it.
- Foster good relations between people who share a relevant protected characteristic and those who do not share it.

The general duty is assisted by documenting decision-making and by keeping results of activities, through monitoring and review arrangements. This is partially evidenced by completing EIAs.

The Met therefore has to consider the impact of **policy** and **procedures** on the protected characteristics listed under the Act of groups of persons, which are set out below. All Met policies are developed/ reviewed using a consultative approach involving relevant internal and external stakeholders. Both positive and negative aspects that arise during the equality assessment are to be recorded. Once published the impact of policy and procedures are monitored to identify any emerging issues and the policy itself will be subject to a minimum of a 4-yearly review.

Research and consultation	
Review of research	Organisational or legislative change has been the main driver for amendment following review of this policy. The policy now combines both data and technology assets management. Organisational change has included greater emphasis on application and governance through the information asset ownership (IAO) model, plus replacement of protective security by the introduction of Government Security Classification (GSC) requirements. Regarding legislative change, the new Data Protection Act 2018 (DPA)/ GDPR is the most significant information rights legal shake-up of governance to appear for several years, already having an impact on improving IM best practice in the Met. The Data and Technology Management Policy itself supports the use of Equality Impact Assessments (EIAs) for future ICT systems and their associated data processing capabilities. This recommendation applies where any personal data, special category data [i.e. sensitive personal data] or crime data [defined under the Data Protection Act 2018 (DPA)] held on systems is additionally an identifiable 'protected characteristic' as defined under the Equality Act 2010. In such circumstances, EIAs are to be completed by the system owner/ project manager at an early business approval stage of the system development project. Additionally, a Data Protection Impact Assessment (DPIA) is now a <u>mandatory requirement</u> for any new/ or changed ICT systems holding personal data collections at significant risk of compromise [see DPA section 64]. A DPIA is similar to an EIA and is used to build in 'privacy by design' at an early stage of the ICT systems project. The use of technical, administrative or behavioral controls is an output designed to protect individual privacy rights. Therefore, completion of both an EIA <u>and</u> DPIA at the beginning of a new project will be particularly beneficial in teasing out any equality impacts, privacy and security requirements, so that they can be adequately addressed in line with Data and Technology Management Policy and best practice.
Internal consultation	Besides other units within Met HQ Strategy & Governance – Information & Insight [the Data Office], consultation includes Transformation Directorate – Met Change 2025 Programme model; Digital Policing (DP); Directorate of Professional Standards (DPS); Department of Legal Services (DLS); Met Vetting Unit; Head of Safety

	and Health Risk Management Team; Property Services Directorate (PSD); Protective Security; the Finance Business Partner, Directorate of Commercial Services and Met End Users/ Practitioners [including BCU/ MO units].
External consultation	External consultation was carried out with Mayor's Office for Policing & Crime (MOPAC) – Directorate of Audit, Risk & Assurance (DARA); Police Federation, Superintendent's Association and Police Staff Trade Union Side.
Protected characteristics (Equality Act 2010)	
Summary of Equality Impact assessment	In certain circumstances, operational policing justifies legal collection of personal data, special category [sensitive personal] data and crime data, including that concerning protected characteristics. Such data will be protected under the Data Protection Act 2018, in addition to the Equality Act 2010. Justification for the collection and storage of this data is given below. Where data is collected and stored, including for internal HR purposes, this will be in compliance with records management (RM), Management of Police Information (MoPI), Data Protection Act (DPA) and GDPR. It will only be processed if there is a legal public interest to do so and it does not infringe individual equality, diversity or privacy rights. This may include the use and profiling of anonymized data when it meets a legitimate aim, such as for improved safeguarding or public protection purposes. Internal HR processes regarding MPS personnel will also legitimately collect and process such personal/ special category data for employment purposes.
Age	Police information [e.g. crime data] – collection/ retention of date of birth/ age data can be relevant/ legitimate in crime investigations. It will constitute personal data under the DPA 2018 as well as being a protected characteristic. A benefit is that disproportionality and trends can be measured / addressed through Met statistical analysis to ensure issues affecting certain age groups are addressed e.g. children and vulnerable / older adults. Other Met information – age is relevant for some data held for legitimate employment purposes on Met personnel, for example, for pay and pension provision, vetting and for recruitment purposes. In relation to the latter, equal opportunities data collection ensures that recruitment processes remain compliant with the Equalities Act 2010.

Deaf / disability	Police information [e.g. crime data] – collection/ retention of deaf/ disability data is unusual in relation to crime investigations. It is more likely a protected characteristic encountered on first contact with the public, when adjustments and assistance is required. It will constitute personal data under the DPA 2018/ GDPR and possibly special category data under the Act if medical records are involved. Because of the individual specific disability requirements involved, it is unlikely that specific EA monitoring is necessary. Other Met information – As an Equal Opportunities employer, the Met lawfully holds personal data on disabled staff, for example, so as to make reasonable adjustments for workplace access/ use of equipment in order to meet individual needs.
Gender reassignment	Police information [e.g. crime data] – collection / retention of gender reassignment data is not necessary in most crime investigations. The main exception would be transphobic hate crimes. If recorded it will constitute special category data under the DPA 2018/ GDPR. Specific EA monitoring may involve ICT systems development in the future regarding this protected characteristic. Other Met information – The Met has issued internal policies to cover Met personnel who have or plan to transition. This ensures fair treatment and counters possible discrimination in the workplace. It also covers confidentiality requirements of HR records. The DPA 2018/ GDPR also provides adequate legal protection additional to policy and other legal requirements.
Pregnancy and maternity	Police information [e.g. crime data] – collection/ retention of pregnancy/ maternity is necessary should the police feel the individual is vulnerable and safeguard measures need to be applied. If recorded It will constitute special category data under the DPA 2018/ GDPR as it concerns medical details. Other Met information – Female police officers/ police staff are eligible for maternity leave and fathers, paternity leave, in accordance with HR Policy detailing employment rights/ police regulations. Clearly, it is not lawful to treat pregnant staff less favourably compared to others due to their condition, in respect of pay, recruitment or other rights. The DPA 2018/ GDPR provides adequate legal protection in addition to policy and employment rights.
Marriage/ Civil Partnership	Police information [e.g. crime data] - collection/ retention of marriage/ civil partnership status is sometimes a relevant factor recorded by police during an investigation. Investigation of domestic abuse allegations may require recording of such data, to identify all parties and to establish parental responsibilities for the safeguarding of children found on the premises. It will constitute personal data under the DPA 2018 as well as being a protected characteristic. Other Met information - Internally, marital/ partnership status can be

	recorded as part of HR records, but only for specific purposes e.g. so that pensions can be correctly paid out to a surviving spouse. The DPA 2018/ GDPR provides adequate legal protection in addition to policy and employment rights.
Race or ethnic origin	Police information [e.g. crime data] - To be justifiable the collection/ retention of any race/ ethnic origin data must be for a clear 'policing purpose', as it constitutes special category data that needs protection under the DPA 2018. Some areas of statistical data collection, particularly stop / search results, remain significantly contentious and attract political scrutiny. Only by measuring such protected characteristic data anonymously, however, can the Met improve their processes and build on any gains for a more positive police and community interaction. Other Met information – Although it has taken a number of years, the proportion of police officer/ staff recruits applying from BME backgrounds has been encouraging as the numbers joining has risen steadily. The DPA 2018/ GDPR provides adequate legal protection, in addition to policy and employment rights for individuals [Met personnel and applicants] declaring their racial or ethnic origin.
Religion or belief	Police information [e.g. crime data] – Collection/ retention of data relating to religion or belief is occasionally a factor in crime recording, usually associated with the rise in hate crime concerning various religious groups. It is important to bear in mind that this is a protected characteristic, which also represents special category data under the DPS 2018/ GDPR. Other Met information – Internally this protected characteristic is rarely recorded, except on recruitment as part of equal opportunities monitoring. The DPA 2018/ GDPR provides adequate legal protection, in addition to policy and employment rights for individuals [Met personnel and applicants] declaring their religion or belief origin.
Sex [Gender]	Police information [e.g. crime data] - Collection/ retention of data relating to gender is not required in relation to most crime investigations. However, as women are disproportionately the victims in certain crimes [sexual offences, harassment and domestic abuse], it is important that measuring such protected characteristic data anonymously, can help the Met improve their processes to improve victim care / outcomes. Sex (gender) is personal data under the DPA Act 2018/ GDPR. Other Met information –The Met actively promotes / monitors the equality duty to ensure equal employment rights are applied in practice irrespective of gender. The DPA 2018/ GDPR provides adequate legal protection, in addition to policy and employment rights for individuals [both Met personnel and applicants].

Sexual orientation	Police information [e.g. crime data] – Collection/ retention of data relating to sexual orientation/ preference is occasionally collected in certain crimes from domestic abuse to hate crimes. Sexual orientation is special category data under the DPA 2018 / GDPR. Other Met information – The Met actively promotes/ monitors the equality duty to ensure equal employment rights are applied in practice irrespective of sexual orientation. The DPA 2018/ GDPR provides adequate legal protection, in addition to policy and employment rights for individuals [both Met personnel and applicants].
Other issues	The Met will record data in line with MoPI policing [law and order] purposes including that required for public protection / safeguarding / benefit of children, vulnerable adults including marginalised groups in society e.g. rough sleepers and sex workers.
Monitoring	
12 month implementation plan	Audit processes from DARA to HMICFRS of specific MPS systems and processes will help identify the compliance of this policy. Information security, data protection and data quality are regularly scrutinised, where audit trail integrity, legal responsibility and data asset governance also feature.