

REQUEST FOR DMPC DECISION – PCD 340**Title: Met Integrated Policing System (MiPS) Full Business Case****Executive Summary:**

This Full Business Case recommends the procurement of a Commercial Off the Shelf integrated policing solution, to be known as the Met Integrated Policing Solution (MiPS) in line with the Police and Crime Plan 2017, which states:

“We will also invest in other systems to improve the MPS’ ability to investigate crime, through MiPS (Met Integrated Policing Solution), which will bring together information from Custody, Investigation, Intelligence and Prosecution, replacing a number of ageing existing systems. This will allow access and input of information through one interface and provide remote access for officers and staff, improving the quality of investigations and providing smart ways of working, irrespective of location or device”

The purpose of the MiPS project is to deliver an integrated core policing IT solution, which will enable the transformation of operational policing services within the Metropolitan Police Service by replacing standalone legacy applications and building on the investment already made in mobile devices.

This integrated IT policing solution will deliver a single, unified, operational policing system that manages joined-up information and end-to-end police business processes in relation to all Investigation, Intelligence, Custody and Prosecution (case) management.

The Met’s ambition to secure an integrated IT platform is entirely in step with the other 42 forces in England and Wales. The Met is currently one of only three regional forces not benefiting from an integrated IT platform.

Recommendation:

The Deputy Mayor for Policing and Crime is recommended to approve

1. Award of contract to the Preferred Bidder as soon as practicable after the mandatory standstill period.
2. Delegation of responsibility to the MPS Commercial Director for contracts with other suppliers that are within the scope of this Full Business Case including award of Data Migration Services with a total contract value of £1.5m.
3. Capital funding of £106.737m from the approved Capital Plan for this project.
4. That the Capital Plan is re-profiled according to the spend profile in Table 12.
5. Revenue funding of £6.774m p.a. and one-off revenue of £500k as part of the Digital Policing Medium Term Financial Plan.
6. That the relevant Revenue budgets are amended accordingly as detailed in Table 14.

And to note:

7. That the MPS Commercial Director shall notify all bidders of the award decision having first informed MOPAC of the identity of the Preferred Bidder.
8. That capital funding of up to £2.968m across financial years 2022/23 to 2027/28 will be required from the Capital Programme in future years as the current programme only covers up to financial year 2021/22.
9. That the total projected revenue spend from 2018/19 to 2027/28 is £60.7m, a saving of £2.3m against the total costs (£63m) provided for in the Medium Term Financial Plan.
10. That the total cashable benefits of £81m, plus the cost savings of £2.3m are £21.7m less than the total savings (£105m - £15m a year from 2021/22) currently assumed in the MTFP. However, there are quantitative non-cashable benefits that are expected to be released through productivity gains as a result of new Target Operating Models. Delivery of cashable benefits for Intelligence & Investigation and productivity gain related benefits are the accountability of the SRO for Programme 4.
11. That the SRO for Programme 4 is accountable for delivering the indirect quantitative cashable benefits that this project enables associated with the delivery of Target Operating Models, and that commitment will be built into the Medium Term Financial Plan.
12. That the SRO for Programme 9, supported by Digital Policing, is responsible for delivering the benefits associated with decommissioning legacy systems, providing there are sufficient funds in the capital plan.
13. That the cost of borrowing capital is allowed for in the Medium Term Financial Plan.
14. That further assurance processes will be arranged as required to help ensure continuous validation of the activities to deliver a successful outcome and will be reported to PIB and IAB as appropriate.

Deputy Mayor for Policing and Crime

I confirm I have considered whether or not I have any personal or prejudicial interest in this matter and take the proposed decision in compliance with the Code of Conduct. Any such interests are recorded below.

The above request has my approval.

Signature

Seamus Warden

Date 05/04/18

PART I - NON-CONFIDENTIAL FACTS AND ADVICE TO THE DMPC

Decision required – supporting report

1. Introduction and background

- 1.1. The Metropolitan Police Service currently operates numerous information technology applications that do not optimally support front-line policing. They are expensive to maintain, inefficient to use and do not enable officers and staff to deliver high quality criminal justice outcomes to the people of London. In the foreseeable future there is a possibility of system failure resulting in data quality and availability issues, impacting upon operational delivery. These dated applications are not able to adequately support vulnerable people, protect the interests of victims or manage risk. From April 2019, the national Home Office nominal database will no longer interface to the Metropolitan Police Service's custody application; a replacement solution must therefore be deployed by that date to avoid operational impact.

2. Issues for consideration

- 2.1. In order for the Metropolitan Police Service to be able to deliver effective policing services to London, with rising demand and a reduced number of officers, the only option is for the organisation to transform and improve the way that information is shared and managed, bringing our information together and avoiding rekeying – MiPS will deliver this capability. MiPS is therefore a core component of the digital transformation that will radically change the way in which all staff and officers discharge their duties.
- 2.2. Benefits are wide ranging and have high impact. London's communities will enjoy improved criminal justice outcomes; the Met's officers and staff will be accessing digital capabilities that are at the forefront of police technology.

3. Financial Comments

- 3.1. The total cost to implement MiPS is £109.705m in capital.
- 3.2. Ongoing revenue costs for MiPS will be £6.774 which is part of the Digital Policing revenue budget.

4. Legal Comments

- 4.1. The Mayor's Office for Policing and Crime (MOPAC) is a contracting authority as defined in the Public Contracts Regulations 2015 (the Regulations). All awards of public contracts for goods and/or services value at £181,302 or above must be procured in accordance with the Regulations.

5. Equality Comments

- 5.1. An Equalities Impact Assessment (EIA) was completed as part of the production of this business case to identify potential positive and negative equality impacts towards people who fall within the protected characteristics under the Equalities Act 2010. Access considerations were documented and taken into account. The Strategic Diversity & Inclusion Unit were consulted as part of this EIA and FBC.

6. Background/supporting papers

- 6.1. Report

Public access to information

Information in this form (Part 1) is subject to the Freedom of Information Act 2000 (FOIA) and will be made available on the MOPAC website following approval.

If immediate publication risks compromising the implementation of the decision it can be deferred until a specific date. Deferral periods should be kept to the shortest length strictly necessary.

Part 1 Deferral:

Is the publication of Part 1 of this approval to be deferred? YES

If yes, for what reason: Commercial Confidentiality

Until what date: 20 April or as advised by MPS Commercial

Part 2 Confidentiality: Only the facts or advice considered as likely to be exempt from disclosure under the FOIA should be in the separate Part 2 form, together with the legal rationale for non-publication.

Is there a **Part 2** form – YES

It is recommended that the information in the Part 2 form not be published since if a request for this information was made under the FOIA, it is likely that it would be exempt from disclosure under the following sections for the FOIA:

Section 43 Commercial Interest

Date at which Part 2 will cease to be confidential or when confidentiality should be reviewed: 31st October 2020

ORIGINATING OFFICER DECLARATION

	Tick to confirm statement (✓)
Head of Unit: The Chief Finance Officer has reviewed the request and is satisfied it is correct and consistent with the MOPAC's plans and priorities.	✓
Legal Advice: The MPS legal team has been consulted on the proposal	✓
Financial Advice: The Strategic Finance and Resource Management Team has been consulted on this proposal.	✓
Equalities Advice: The Workforce Development Officer has been consulted on the equalities and diversity issues within this report.	✓

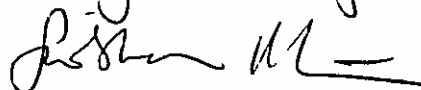
OFFICER APPROVAL

Chief Executive Officer

I have been consulted about the proposal and confirm that financial, legal and equalities advice has been taken into account in the preparation of this report. I am satisfied that this is an appropriate request to be submitted to the Deputy Mayor for Policing and Crime.

CFO with delegated authority:

Signature



Date 5/4/2018



Met Integrated Policing System (MiPS) Full Business Case

MOPAC Investment Advisory Board 22nd March 2018

Report by Duncan Ball on behalf of the Deputy Commissioner

Part 1 – This section of the report will be published by MOPAC. It is classified as OFFICIAL – PUBLIC

EXECUTIVE SUMMARY

This Full Business Case (FBC) recommends the procurement of a Commercial Off the Shelf (COTS) integrated policing solution, to be known as the Met Integrated Policing Solution (MIPS).

The purpose of the MIPS project is to deliver an integrated core policing IT solution, which will enable the transformation of operational policing services within the MPS by replacing standalone legacy applications and building on the investment already made in mobile devices.

The Police & Crime Plan 2017 states: *“We will also invest in other systems to improve the MPS’ ability to investigate crime, through MiPS (Met Integrated Policing Solution), which will bring together information from Custody, Investigation, Intelligence and Prosecution, replacing a number of ageing existing systems. This will allow access and input of information through one interface and provide remote access for officers and staff, improving the quality of investigations and providing smart ways of working, irrespective of location or device”*

This integrated IT policing solution will deliver a single, unified, operational policing system that manages joined-up information and end-to-end police business processes in relation to all Investigation, Intelligence, Custody and Prosecution (case) management.

The Met’s ambition to secure an integrated IT platform is entirely in step with the other 42 forces in England and Wales. The Met is currently one of only three regional forces not benefiting from an integrated IT platform.

Recommendations

The Deputy Mayor for Policing and Crime, via the Investment Advisory Board (IAB), is asked to approve:

- 1. Award of contract to the Preferred Bidder as soon as practicable after the mandatory standstill period.**

2. **Delegation of responsibility to the MPS Commercial Director for contracts with other suppliers that are within the scope of this Full Business Case including award of Data Migration Services with a total contract value of £1.5m.**
3. **Capital funding of £106.737m from the approved Capital Plan for this project.**
4. **That the Capital Plan is re-profiled according to the spend profile in *Table 12*.**
5. **Revenue funding of £6.774m p.a. and one-off revenue of £500k as part of the Digital Policing Medium Term Financial Plan.**
6. **That the relevant Revenue budgets are amended accordingly as detailed in *Table 14*.**

And to note:

7. **That the MPS Commercial Director shall notify all bidders of the award decision having first informed MOPAC of the identity of the Preferred Bidder.**
8. **That capital funding of up to £2.968m across financial years 2022/23 to 2027/28 will be required from the Capital Programme in future years as the current programme only covers up to financial year 2021/22.**
9. **That the total projected revenue spend from 2018/19 to 2027/28 is £60.7m, a saving of £2.3m against the total costs (£63m) provided for in the Medium Term Financial Plan.**
10. **That the total cashable benefits of £81m, plus the cost savings of £2.3m are £21.7m less than the total savings (£105m - £15m a year from 2021/22) currently assumed in the MTFP. However, there are quantitative non-cashable benefits that are expected to be released through productivity gains as a result of new Target Operating Models. Delivery of cashable benefits for Intelligence & Investigation and productivity gain related benefits are the accountability of the SRO for Programme 4.**
11. **That the SRO for Programme 4 is accountable for delivering the indirect quantitative cashable benefits that this project enables associated with the delivery of Target Operating Models, and that commitment will be built into the Medium Term Financial Plan.**
12. **That the SRO for Programme 9, supported by Digital Policing, is responsible for delivering the benefits associated with decommissioning legacy systems, providing there are sufficient funds in the capital plan.**
13. **That the cost of borrowing capital is allowed for in the Medium Term Financial Plan.**
14. **That further assurance processes will be arranged as required to help ensure continuous validation of the activities to deliver a successful outcome and will be reported to PIB and IAB as appropriate.**

Non-confidential facts and advice to the Deputy Mayor for Policing and Crime

Introduction and background

15. The Metropolitan Police Service currently operates nine different information technology applications that do not adequately support front-line policing. They are expensive to maintain, inefficient to use and do not enable officers and staff to deliver high quality criminal justice outcomes to the people of London. In the foreseeable future there is a possibility of system failure resulting in data quality and availability issues, impacting upon operational delivery. These dated applications are not able to adequately support vulnerable people, protect the interests of victims or manage risk. From April 2019, the national Home Office nominal database will no longer interface to the Met's custody application; a replacement solution must therefore be deployed by that date to avoid operational impact.
16. All but two forces in England and Wales have already procured an integrated IT solution of this type and are seeing significant operational benefit due to its use, such as:
 - a. Operational officers spending less time engaged in data entry tasks and more time being visible in their communities.
 - b. Faster access to intelligence, facilitating quicker and more informed decision making to better manage risk.
 - c. A more coherent approach to demand management, tasking officers through the integrated IT platform to make better use of police time.
17. To de-risk delivery of this project, the solution to be procured is one of those COTS applications already in live use in a UK police force. The MPS is working closely with these forces to capture technical lessons and those related to business change in order to mitigate risks to delivery for London. Due to the scale of the project, further risk mitigation is provided through a controlled implementation on a module-by-module basis over an 18-month period from April 2019.
18. Commitment to this project has been made by the Mayor in the Police and Crime Plan 2017.
19. This paper follows the structure of the Part 2 Full Business Case. It sets out the:
 - Strategic Case for the project, detailing the reasons why this is needed
 - Economic Case, which identifies the best value for money option (considering both qualitative/operational and quantitative factors)
 - Commercial Case, which explains the procurement method and analysis of bids
 - Financial Case, which sets out how the project will be funded and its affordability
 - Management Case, which explains how the project will be delivered.

Strategic Case

20. In order for the MPS to be able to deliver effective policing services to London, with rising demand and a reduced number of officers, the only option is for the organisation to transform and improve the way that information is shared and managed, bringing our information together and avoiding rekeying – MiPS will deliver this capability. It is one of the most significant and ambitious transformation projects in the One Met Model 2020 (OMM) change portfolio. An integrated end-to-end policing solution is critical to the success of the OMM Blueprint to deliver efficient and effective operational services within

the MPS and to deliver the savings required. The MiPS project therefore provides key capabilities for other OMM projects to leverage, particularly those relating to new target operating models and information futures.

MPS Legacy IT Systems

21. The legacy IT applications in use in the MPS do not optimally support operational requirements. This is especially so in relation to use of intelligence and the effective management of risk. These legacy applications have been developed using different technologies and suppliers, often hosted on different platforms. This has resulted in a large number of stand-alone systems with little integration between them. They are difficult and expensive to maintain, inflexible to change and no longer fit for purpose to support modern policing in a global city.

The National Picture

22. The Met's ambition to secure an integrated IT platform is entirely in step with the other 42 forces in England and Wales. The Met is currently one of only three regional forces not benefiting from an integrated IT platform. The project team have spent time with colleagues across the country, seeing the benefits of an integrated solution and understanding the opportunities that such applications present.
23. The remaining two police forces are awarding contracts imminently. This will leave MPS as the only force using the NSPIS Custody system. As the Home Office strategy is to replace PNC and PND with a new national solution (NLEDS) without an interface between NLEDS and NSPIS, this would require development of a new interface specifically for use by the MPS. Implementing MiPS to the current plan will avoid these costs. The MPS will require an interface to NLEDS in order to facilitate shared data with other police forces, which MiPS will provide.

Business Needs

24. Policing the Capital with the legacy IT applications identified above is a considerable constraint for an organisation that has a stated vision of making London the safest global city. The nature and complexity of the work undertaken by the Met is changing. The need to operate with a reliable, modern IT capability is clear. The MiPS solution will deliver a single, integrated, operational policing system that manages information and end-to-end policing processes in relation to all investigations, detention (custody), intelligence and prosecution (case) management.

Intelligent Decision-Making: A Data Driven Organisation

25. The Commissioner has articulated a very clear objective that the MPS must evolve to being a truly data-driven organisation. The data at the organisation's disposal is vast and it is essential that the MPS takes the steps necessary to organise this information to better understand its potential. MiPS is a core component of achieving that goal. In parallel, partner agencies across the public and third sector have a need to work with the Met and use crime data to better target their own activities to meet shared objectives. Working towards an agenda of transparency and trust between partner agencies is key – sharing accurate information that acts as an enabler to delivering improvements in public service. For example, where intelligence requests are received from other forces, time is saved as there will no longer be a need to search and retrieve info from multiple separate, unlinked systems; person profiles will be very quick to obtain and send out.

Meeting Strategic Expectations on Safeguarding London's Most Vulnerable People

26. Recent criticisms of the MPS have often focused on whether the best use is made of data and intelligence within the service.

27. One of the most significant examples of this is within the context of safeguarding London's most vulnerable people. Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS), in their National Child Protection Inspection, identified that significant opportunities exist to make better use of data and technology:

"The lack of connection among the IT systems, databases and spreadsheets that the MPS uses to record such analyses exacerbates this problem. As a result, information on victims, offenders and risks is too often kept in isolated pockets across the force".
(HMICFRS, November 2016).

28. This is an issue that can be seen in other parts of the MPS, particularly where vulnerability needs to be identified and acted upon.

Police and Crime Plan

29. The Mayor's Police and Crime Plan 2017 – 2021 identifies amongst other, three key priorities including Tackling violence against women and girls, keeping children and young people safe and standing together against hatred, intolerance and extremism.:

30. Within the context of the MPS' ambition to become a data-driven organisation, it is clear that each of these priorities requires an intelligence-led, targeted response. There is a clear need to build a coherent data picture, which can drive effective decision making, to protect the most vulnerable in our communities.

Putting Victims at the Heart of the Criminal Justice Service

31. Caring for victims is a clear priority for MOPAC and for the MPS' officers and staff. Building up a rich intelligence picture is essential to piecing together instances of, for example, truancy, mental health crisis and repeat offending – the sum total of which is vital evidence to identify vulnerability and mitigate risk. The Mayor has a stated commitment to increase the protection of victims and vulnerable people, and the provision of an integrated policing system will ensure a holistic view of victims that will enable officers to tailor their approach and provide clear information on the progress of investigations, whilst also engaging victims as key partners in the investigation journey. This cannot be achieved without MiPS.

Case Study

- PC Shah is despatched to attend an immediate call at Avenue Road. A neighbour has called police, having heard a female screaming in the flat above.
- The despatcher has only had to search a **single database** to identify any pertinent risks that should be brought to the attention of PC Shah.
- She is advised that a baseball bat has previously been seen behind the front door, so **proceeds with caution**.
- Mrs Jones states she has been assaulted by her husband and is visibly injured. Their daughter is also present.
- PC Shah arrests Mr Jones and records details on her **mobile device**, directly into MiPS.
- PC Shah returns to the police station.
- The **custody officer already has details of the incident** in MiPS and creates the custody record accordingly. Mr Jones is already known to police, all of that person data is pulled into the custody record.
- The same person, location, event details are available for PC Shah to quickly generate an anti-social behaviour and vulnerable persons record.
- There is almost **no re-keying of data**.
- A detailed, accurate picture of the incident is recorded, meaning that Mrs Jones will receive the support she needs.

Further Enabling the Met's Mobile Ambitions

32. Through the Smarter Working Programme significant progress has been made to mobilise the Met's workforce. Officers are now spending more time in London's communities, with technology that is removing the need to continually return to a police station. Looking ahead, the aspiration is clear: MiPS will be mobile. The desktop applications identified above are already, in many cases, well beyond their useful life with extensive work arounds and hand-crafted add-ons needed to make them accessible on the move. By definition the mobile applications which work off this technology are simply not viable over the medium to long term. The significant investment that has rightly been made in deploying over 20,000 mobile devices to front line personnel will quickly become obsolete if a supporting investment in mobile software, through MiPS, is not also made.
33. An integrated IT platform services these business needs in a way that the organisation's existing disparate IT infrastructure simply cannot. In addition to bringing all existing capabilities into a new application MiPS will introduce new functionality that is not currently available to the Met.

Economic Case

34. The quantitative and qualitative benefits of the preferred options are listed below;

35. Quantitative - cashable - direct:

i.e. direct cash savings to the MPS realised directly through the implementation of this project

- The direct release of FTEs from Investigation, equating to £7.4m over 10 years
- Reduced spend on stationery costs, saving £185k per year and £1.3m over 10 years
- Total savings as above of £8.7m over 10 years

Quantitative - cashable - indirect:

i.e. cash savings to the MPS enabled by this project but dependent on the implementation of other projects, at additional costs, to be realised

- The release of FTEs from Intelligence, equating to £31.6m over 10 years
- Savings of £40.7m of revenue over 10 years through decommissioned systems
- Total savings as above of £72.3m over 10 years

Quantitative - non-cashable:

i.e. improvements that can be measured but do not directly release cash

- A large number of small efficiency savings that in the aggregate represent the release of a significant amount of 'productive time'

36. Qualitative:

i.e. benefits which cannot readily be measured

- Significant qualitative improvements in key operational policing areas that directly support the priorities identified in the Mayor's Police and Crime Plan including.
- The enhancement of service to the public through the improved identification and management of risk
- The empowerment of MPS officers and staff to discharge their duties from a position of knowledge through enhanced quality and access to critical information.

- Mitigation of risks to the MPS resulting from slow and less reliable systems which require increasing down time and reduced availability, and mitigating the increasing costs of maintenance and support.

37. The total investment to deliver these benefits is £170.9m (£109.7m Capital, £60.7m Revenue and £0.5m one-off Project Revenue).

Commercial Case

38. MiPS procurement has adopted a legally compliant route to market for the Preferred Bidder contract, delivering against organisational requirements. It has been run under the Competitive Procedure with Negotiation (CPN) route.

39. Contracts with other suppliers that are within the scope of this Full Business Case have been/will be let by legally compliant routes to market.

Financial Case

40. The Financial Case outlines the cost of implementing MiPS, identifying:

- a) The capital and revenue costs
- b) How the project is funded.
- c) How it fits within the Medium Term Financial Plan (MTFP).

41. The capital programme includes £110m for 2018/19 – 2020/21 to cover Capital costs. The total cost to implement MiPS is £109.737m in capital.

42. Ongoing revenue costs for MiPS will be £6.774 which is part of the Digital Policing revenue budget.

Capital costs for the programme exceed the capital funding reserves and therefore borrowing will be required. The existing Medium Term Financial Plan (MTFP) has made full provision for the capital and revenue costs (including borrowing) of this project.

Management Case

43. This project will continue to be delivered in line with the governance processes of the One Met Model as part of Programme 4: Transforming Investigation and Prosecutions.

44. The project has mapped its stakeholders and communications and stakeholder engagement will be undertaken against a detailed plan. This will be based on a Strategy and Approach approved by the Project Board and supported by all levels of management, which clearly sets out how the project will communicate tailored messages to different audiences using appropriate communication channels.

45. The MPS will de-risk the MiPS delivery in 4 key areas:

- **Staged, Controlled Delivery:** Delivery is divided into defined, bundled capability rendered against technology, process fit and readiness of the operational rollout plan to frontline officers and staff.
- **Core Build:** The use of a "Core Build", followed by staged delivery of Custody, Case, Intelligence, and investigation.
- **Business Process:** Configuration of MiPS will only start when the business processes have been agreed and signed off, and test gates will be formalised.

- **System Integration:** The set-up of an internal System Integration team, to direct and manage the end-to-end technical delivery, data interfaces, data migration and rollout of the system and business transformation.
46. Business Change activities are designed to support individuals so that they are willing and able to behave differently, and to deliver the desired benefits of any business change. A structured approach to business change management will be needed, encompassing extensive business engagement (so people are willing to adopt the change) and business readiness activities (so they are able to adopt the change).
 47. The MiPS Training Strategy sets out a strategic context, purpose and approach to the planning and delivery of training. It describes how MiPS Training will be developed for maximum impact and minimum abstraction in such a way as to mitigate threat or risk to service levels across the organisation.
 48. The project will define and keep current a comprehensive Benefits Realisation Plan that will set out which benefits will be realised when, the project dependencies required to realise them, appropriately scheduled benefits reviews and responsibilities for monitoring of agreed measures or direction of travel, in line with portfolio standards.
 49. The Project falls within the Assurance Framework for the OMM Portfolio. This framework has three dimensions; First Line Self Assurance, Second Line Internal Assurance and Third Line- Independent external assurance which has been conducted via the Infrastructure and Projects Authority (IPA) OGC Gateway process. An OGC review was undertaken in January 2018 as part of this third line assurance.
 50. In addition to the recent assurance detailed above, the MiPS project will be required to undertake further assessments of a similar type over the remaining duration of the project, both as part of the routine gate review processes and through internal and external assurance reviews.
 51. The intention is to undertake a project evaluation review (PER) and post implementation review (PIR) in accordance with project management best practice. The PER appraises how well the project was managed and whether or not it delivered to expectations. This could take the form of an independent PER report at the conclusion of the project; outputs will include a Project Closedown Report and Lessons Learned Log. The PIR ascertains whether the anticipated benefits have been delivered. Given that MiPS is primarily a system replacement and enabling project, the timing and scope of the PIR will need to reflect that other programmes will deliver some of the benefits enabled by MiPS and the timescales in which these benefits will be realised.

Legal Comments

52. The Mayor's Office for Policing and Crime (MOPAC) is a contracting authority as defined in the Public Contracts Regulations 2015 (the Regulations). All awards of public contracts for goods and/or services value at £181,302 or above must be procured in accordance with the Regulations.

Equality Comments

53. An Equalities Impact Assessment (EIA) was completed as part of the production of this business case to identify potential positive and negative equality impacts towards people who fall within the protected characteristics under the Equalities Act 2010. Access considerations were documented and taken into account. The Strategic Diversity & Inclusion Unit were consulted as part of this EIA and FBC.

Privacy Comments

54. Due consideration has been given to the obligations that data protection legislation, particularly the Data Protection Act 1998, place on the MPS. The MPS takes data protection responsibilities extremely seriously, recognising that all data held for a policing purpose must be subject to necessary governance and controls. The legacy systems are difficult to make compliant with data privacy legislation due to their age, so MiPS is important to ensure that the MPS is able to comply with new regulatory requirements as they emerge. The MiPS Data Privacy Impact Assessment has been attached as Annex 1.

Real Estate Implications

55. There are no real estate implications for this project that are not covered by other projects and initiatives.

Environmental Implications

56. An environmental impact assessment has been carried out as part of the production of this business case, and all indicators are either "Lower" or "No Impact".

Background/supporting papers

57. Supporting appendices available and suitable for publication;
Annex 1: MiPS Data Privacy Impact Assessment

Part 2 – This section refers to the details of the Part 2 business case which is NOT SUITABLE for MOPAC Publication.

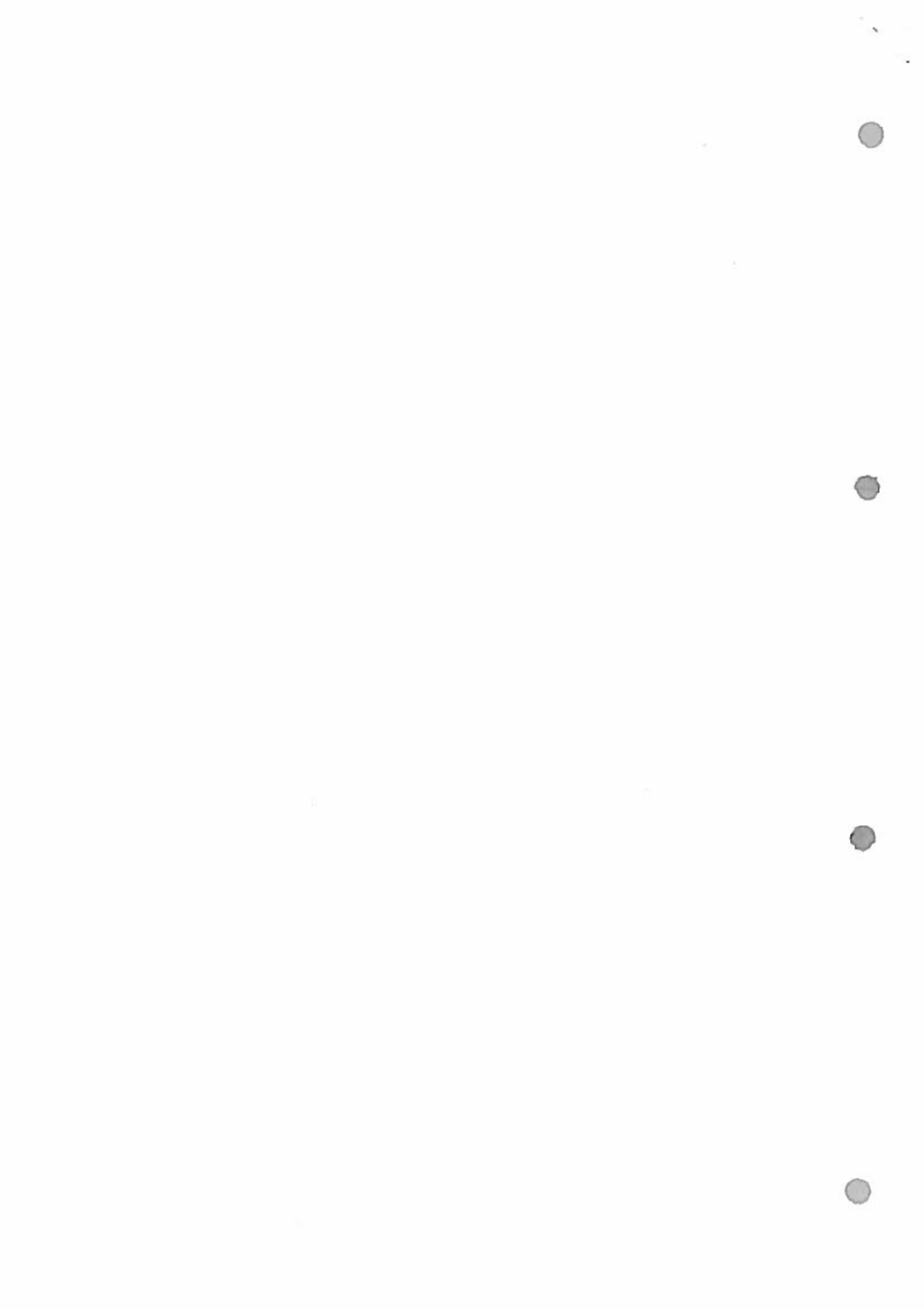
The Government Security Classification marking for Part 2 is:
OFFICIAL-SENSITIVE [COMMERCIAL]

Part 2 of Met Integrated Policing System (MiPS) Full Business Case is exempt from publication for the following reasons:

Exempt Under Article 2(2)(a),(b),(c) of the Elected Local Policing Bodies (Specified Information) Order 2011.

The relevant section under the FOIA that would exempt this information from disclosure is Commercial Interest Section 43, Legal Professional Privilege (section 42), Data Protection (section 40)

The paper will cease to be exempt until December 2021 or when the project has been completed and handed over into business as usual support, whichever is the later.





TOTAL POLICING

Protective Marking: OFFICIAL - PUBLIC	Publication (Y/N): Y
Title: Met Integrated Policing Solution (MiPS) Privacy Impact Assessment	
Summary: An Impact Assessment addressing the gathering, storage and use of (sensitive) personal data within the MiPS solution	
Branch / OCU: Transformation – Programme 4 (MiPS)	
Date created: March 2018	Review date: Version: 3
Author: Insp K Nilsson	

Contents

1.	<u>Introduction</u>	3
2.	<u>Privacy Impact Screening Questions</u>	5
3.	<u>Data Protection and 'Privacy Law' Assessment</u>	6
4.	<u>Consultation Results</u>	17
5.	<u>Balanced Risk Assessment</u>	18
6.	<u>Implementation of PIA Outcomes Responsibilities</u>	20
7.	<u>Conclusion</u>	21
8.	<u>Privacy Impact Assessment Sign-off</u>	22

Appendices

A	23
B	24
C	25

1. Introduction

The Met Integrated Policing Solution (MiPS) is a digital transformation project that will radically change the way in which all staff and officers discharge their duties. It underpins the Met's vision of being the world's safest global city. It is by far the most significant and ambitious transformation project in the One Met Model 2020 change portfolio. The project will deliver an integrated core policing IT solution, which will transform operational policing services within the MPS and replace existing standalone legacy applications. An integrated end-to-end policing solution is a critical enabler to the delivery of efficient and effective operational services for the MPS.

The Metropolitan Police Service (MPS) currently operate numerous information technology applications that are unable to support the changing demands for front-line policing. The current applications used to support front-line policing, are unable to communicate and transmit data on one platform. From April 2019, the national Home Office nominal database will no longer interface to the Met's custody application. With this in mind, the MPS intends to introduce MiPS to interface with the national Home Office nominal database to avoid critical operational impact.

The nature and complexity of the work undertaken by the Met is changing. The need to operate with a reliable, modern IT capability is clear. The MiPS solution will deliver a single, integrated, operational policing system that manages information and end-to-end policing processes in relation to all investigations, detention (custody), intelligence and prosecution (case) management. The solution will have a single 'POLE' data store in relation to core policing entities: People, Objects, Locations and Events. The solution will also introduce the concept of the 'Golden Nominal' – a single consolidated view of an intelligence picture, from which risk can be better understood and resources deployed accordingly.

Through the Smarter Working Programme significant progress has been made to mobilise the Met's workforce. Officers are now spending more time in London's communities, with technology that is removing the need to continually return to a police station. Looking ahead, the aspiration is clear: MiPS supports mobile working. The desktop applications currently used to support mobile working still operate on a standalone principle, and therefore, can not facilitate an end-to-end policing process.

MiPS will not change the data collected by the MPS, the use to which this data is put, nor the interactions by which police officers and staff collect that data from the people of London. However, MiPS will enable this data to be entered into a database at the point of collection, meaning that only the minimum amount of data necessary will need to be recorded, in structured fields, forming verified, high-quality records against the correct data subjects. In many critical fields, data entered will be date/time stamped and locked to prevent accidental deletion, or tampering. Data entered at the point of collection will populate custody records, criminal case files, investigation, and intelligence reports.

OFFICIAL - PUBLIC

The MiPS database is fully searchable by authorised personnel. Access to data is restricted by role-based access (RBAC) controls. Meaning that only authorised users are able to log into and access searches and records. In addition, records considered especially sensitive can be further restricted to individuals, or selected groups on a need to know basis, by the means of Access Control Lists (ACLs).

MiPS will maintain full audit logs of every data transaction or search carried out.

Deletion of data from within the MiPS database is compliant with the 2010 guidelines on the Management of Police Information (MOPI), including audit logs where appropriate.

The initial assessment of this system (at page 5) was that no PIA was required. Although the data collected includes criminal records and other information which people may consider private or sensitive, the assessment below was made on the basis that the implementation of MiPS will not change the data collection patterns, or the reasons for that data capture. Existing MPS documentation, such as the MPS Data Protection Standard Operating Procedures and the MPS Fair Processing Notice were deemed sufficient to govern the use of a software upgrade. However, at the request of MOPAC, this PIA has been produced to comply with the very latest guidelines issued by the Information Commissioner's Office, and to address the legislative effect of the General Data Protection Regulations (GDRP) on this specific policing system.

2. Privacy Impact Screening Questions

		Yes	No
Q.1	Will the project involve the collection of new information about individuals?		✓
Q.2	Will the project compel individuals to provide information about themselves?		✓
Q.3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		✓
Q.4	Will the MPS be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		✓
Q.5	Does the project involve the MPS using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		✓
Q.6	Will the project result in the MPS making decisions or taking action against individuals in ways that can have a significant impact on them?		✓
Q.7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.		✓
Q.8	Will the project require the MPS to contact individuals in ways that they may find intrusive?		✓

If the answer to any of the above questions results in a 'yes' then a DPIA is required.

Further advice regarding this screening can be obtained via the Information Law and Security Group.

3. Data Protection and 'Privacy Law' Assessment

European Convention of Human Rights:

Article 8: Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The MPS is a public authority, therefore, is subject to a statutory duty under HRA Article 6(1) not to act inconsistently with a Convention right. The relevant Convention right for the purposes of this processing is Article 8(1) of the Convention.

It is the view of the MPS that Article 8(1) provides limited protection to the criminal and it is not intended to bar lawful and proportionate law enforcement activities. It is for this reason that the MPS believes that the interference with the Article 8(1) rights can be justified under Article 8(2). The purpose is the prevention and detection of crime. This falls squarely within one of the permissible bases for interference in Article 8(2), which refers specifically to the prevention of disorder or crime. However, the MPS recognises that for the interference to be justified it would need to be "*in accordance with the law*" and "*necessary in a democratic society*", within the meaning of Article 8(2).

1. Does this project / initiative address a Social Need? If so, outline it here:

No. MiPS is a replacement of existing MPS recording systems, and will address the same recording needs as these systems have now. These systems include CRIS, CRIMINT+, NSPIS Custody, COPA, AirSpace, EWMS and MERLIN.

2. Are your actions a proportionate response to the social need?

N/A

Common Law Duty of Confidence:

A breach of confidence will become actionable if:

- the information has the necessary quality of confidence;
- the information was given in circumstances under an obligation of confidence; and
- there was an unauthorised use of the information to the detriment of the confider (the element of detriment is not always necessary).

However, there are certain situations when a breach of confidence is not actionable. Those situations are:

1. If a person has provided consent for the processing of their information.
2. If there is a legal requirement to process the information.
3. If it is in the public interest to process the information.

It is the view of the MPS that points 2 and 3 above are applicable for the reasons already outlined in this PIA.

Data Protection Act 1998

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- a) at least one of the conditions in Schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

For the avoidance of any doubt, this system relies on the following definition of policing purpose as defined by the Code of Practice on the Management of Police Information published 14th November 2005 by the Secretary of State for the Home Department:

- a) The protecting of life and property
- b) Preserving order
- c) Preventing the commission of offences
- d) Bringing offenders to justice, and
- e) Any duty or responsibility of the police arising from common or statute law

The Code of Practice further states in paragraphs 4.1.1 – 4.3.1 that:

“...Chief Officers have a duty to obtain and manage information needed for police purposes...[and]...information should be recorded where it is considered that it is necessary for a police purpose...”

It is the view of the MPS that the requirement for this processing to be both fair and lawful is met through the Pressing Social Need outlined in this PIA (please refer to the Introduction and Section 1).

Data Protection Act 1998:

Where the processing, by its very nature, may not be considered as fair or lawful, the MPS relies on the following Sections of the Data Protection Act 1998 when processing this information:

Section 29(1):

- (a) The Prevention or Detection of Crime
- (b) The Apprehension or Prosecution of Offenders

Section 29(2):

- (a) Processed for the purpose of discharging statutory functions
- (b) Consist of information obtained for such as purpose from a person, who had it in his possession of any of the purposes mentioned in subsection (1), are exempt from the subject information provisions to the same extent as personal data processed for any of the purposes mention in that subsection.

It is the MPS' understanding that in the engaging of the above exemption the processing of this data is exempt from:

- The first Data Protection Act Principle (except the need to meet the Conditions in Schedule 2 and 3 of the Act),
- The Subject Access Provisions
- The Non-disclosure Provisions.

Exemption from the Non Disclosure Provisions (by virtue of engaging Section 29(1)(a)(b) & (2)(a)(b))

It is also the understanding of the MPS that by virtue of Section 29(1)(a)(b) & (2)(a)(b), the exemption from the Non-disclosure Provisions allows him and his Chief Officer colleagues to share/ disclose with each other information obtained as part of our policing purposes as this processing is exempt from the following:

- The first Data Protection Act Principle (except the need to meet the Conditions in Schedule 2 and 3 of the Act);
- The Second, Third, Fourth and Fifth Data Protection Principles;
- The right to prevent processing likely to cause damage or distress (Section 10); and
- The right to rectification, blocking, erasure or destruction (Sections 14(1) to (3)).

When processing this information, the MPS seeks to rely on the following Schedule 2 and 3 Conditions:

Schedule 2:

Paragraph 5(b): the processing is necessary for the exercise of any functions conferred on any person by or under any enactment.

Paragraph 5(d): the processing is necessary for the exercise of any functions of the public nature exercised in the public interest by any person.

Paragraph 6: the processing is necessary for the purposes of legitimate interests pursued by the data controller, except where the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Schedule 3:

Paragraph 7(1)(b): the processing is necessary for the exercise of any functions conferred on any person by or under any enactment.

Paragraph 10: The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph:

Statutory Instrument 2000/ 417:

1(1) The processing—

- (a) is in the substantial public interest; .
- (b) is necessary for the purposes of the prevention or detection of any unlawful act; and
- (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

(2) In this paragraph, “act” includes a failure to act.

10. The processing is necessary for the exercise of any functions conferred on a constable by any rule of law. The legal framework and existing body of guidance in which the MPS relies is provided by the following:

- College of Policing Authorised Professional Practice (APP)
- Management of MPS Intelligence Policy
- MPS Intelligence Strategy
- MPS Intelligence Manual
- ACPO (2005) Guidance on NIM, NIM Codes of Practice & NIM Minimum Standard
- The Data Protection Act 1998
- 2010 Guidance on the Management of Police Information
- The MPS Data Protection Standard Operating Procedures (including international data processing compliance standards)
- MPS Information Governance Framework
- MPS Information Management Strategy

- MPS Information Management Policy
- MPS Security Code
- MPS Records Management Manual (including the Review, Retention and Disposal Schedule).

1. How will you tell individuals about the use of their personal data?

The MPS has a mature Information Governance Strategy and Structure in place which incorporates the requirements of the MPS to be open and transparent around the nature in which (sensitive) personal data are to be processed (where possible).

The MPS has a comprehensive Fair Processing Notice (FPN) provided at all Custody Suites and on the MPS internet site. This notice includes full details of how a subject may exercise their Principle 6 rights.

In addition to this, the MPS publishes copies of the information management related policies we follow, as outlined above. This list is currently subject to a review over the next 6-9 months with a dedicated page on 'Privacy' to be created. This will incorporate all information management policies that the MPS follows on one page, including privacy FAQs, copies of all MPS Information Sharing Agreements, Privacy Impact Assessments, ICO DPA Audits and the MPS FPN.

2. Do you need to amend your privacy notices?

The MPS is content that the existing Fair Processing Notice sufficiently covers the intended processing.

3. If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

No. The reasons for this are twofold:

- 1) Consent can be withdrawn by the data subject at any time, thus requiring the MPS to delete the data and limiting the scope in which the MPS can fulfil our policing purposes.
- 2) Obtaining consent would prejudice the purpose in which the data is collected in the first place.

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

The intended processing is in line with the purposes outlined above as-well-as those listed within the [MPS Fair Processing Notice](#) and our notification with the [Information Commissioner's Office](#): Registration No: Z4888193.

1. Have you identified potential new purposes as the scope of the project expands?

No.

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

It is not the intention of the MPS to process exhaustive amounts of personal information on the loose premise that it may be useful now or in the future. This approach would simply grind the Service to a halt by virtue of the eventual need to wade through the vast quantities of data in order to locate the relevant piece of information needed for our purposes. Additionally, the cost to hold data (even using the various cloud solutions) is significant; therefore, the MPS is only interested in processing data that is relevant to our policing purposes.

If at any point any particular data processed is found to be excessive to the purposes of the MPS (i.e. the value of the system in preventing and detecting crimes, for example, is not realised in practice) then this processing will be ceased. The processing will be

subject to periodic yearly review in terms of assessing the value that this product plays in enabling the MPS to meet its policing purposes by the MiPS Data Administration Team.

1 Is the quality of the information good enough for the purposes it is used?

Yes. At the core of the MiPS system is a relational POLE database, adhering to the principle of a "Golden Nominal". A mandatory "search before create" business rule minimises the creation of duplicate nominals. This ensures that data entered is ascribed to the correct subject, and – by use of formatted field entry and validation wherever possible – is both sufficient, relevant, and of the required quality.

2 Which personal data could you not use, without compromising the needs of the project?

MiPS data recording screens are configured to ensure that only the minimum amount of data necessary is gathered to fulfil the relevant policing purpose.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

The MPS are fully aware of the fear around potential damage and distress to the data subject, the organisation and of third parties if the data processed was inaccurate in anyway. This is especially so if the processing of that inaccurate data lead to erroneous decisions being taken. However, the MPS decision making process do not solely rest with the processing of the data in scope for this project / initiative. This data will make up a suite of data that will be processed by the MPS holistically allowing the MPS to fully analyse the circumstances leading up to, and preceding, a criminal event. It would be impossible for the MPS to make an informed decision around an act of criminality based on this data alone. Therefore, checks and balances will naturally occur as a result of this holistic approach to data processing / analysing.

1 If the MPS are procuring new software does it allow us to amend / delete data when necessary?

Yes.

2 How is the MPS ensuring that personal data obtained from individuals or other organisations is accurate?

The MiPS "search before create" business model incorporates the federated searching of numerous MPS and national systems and databases in order to validate personal data prior to system entry.

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

1 What retention periods are suitable for the personal data the MPS will be processing?

The information will be retained in line with our **Retention, Review and Deletion** policy.

2 Are you procuring software that will allow the MPS to delete information in line with our retention periods?

Yes. MiPS is fully compliant with MOPI guidelines. In addition, data may be deleted by suitably authorised personnel. An audit trail will be retained to ensure that deletion is carried out correctly.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The MPS provides full details regarding how a Data Subject can exercise their Principle 6 Rights within the [MPS Fair Processing Notice](#) and [MPS internet site](#).

The MPS has full and comprehensive policies and local work instructions regarding the handling of Subject Access Requests (SARs).

The MPS shall comply with SARs in accordance with the DPA. There are limited exemptions in which the MPS may exercise should the disclosure of information result in any significant harm. For example, Section 29 of the DPA states that personal data are exempt from the subject access provisions where the application of those provisions would be likely to prejudice the prevention and detection of crime or the apprehension of offenders. The MPS may use this

exemption when responding to subject access requests if we feel that the disclosure of information may prejudice these purposes.

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1. Does the project / initiative provide protection against the security risks the MPS has identified?

As stated in the mitigation, MiPS will be hosted within the MPS domain and is subject to existing, stringent security measures. Access will be via HR-verified warrant/pay numbers, with a unique, user-set password. ACLs control access to data deemed particularly sensitive. These security features apply to existing mobile devices. In addition, end-to-end encryption of mobile data will be provided as standard by the supplier as part of the contract.

2. What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Full training will be provided to all police officers and staff, dependent upon need and access level. The training strategy is addressed elsewhere within the MiPS FBC.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data will only be transferred outside of the UK or EEA where it is in line with our Policing Purposes. For example, if the processing identified a terrorist threat to another country or territory. It is the view of the MPS that it would be proportionate to share this information with our international law enforcement colleagues where this would actively lead to the apprehension of an offender and the location of victims. Please refer to the MPS Compliance Standard for International Data Processing for further details.

Miscellaneous Considerations

1. Complaint Handling

Complaints about the use of Personal Information in relation to this project should be handled by the MPS Data Protection and Freedom of Information Officer.

2. Freedom of Information Act 2000 (FoIA)

The MPS shall demonstrate a commitment to openness and transparency regarding this processing, subject to any limitations posed by security or confidentiality requirements.

The MPS is a public authority for the purposes of the FoIA 2000. This means that any information held by the MPS is accessible by the public on written request, subject to certain limited exemptions.

In line with guidance from the ICO, the MPS will place this PIA and other associated documents on our FoIA Publication Scheme, so the public can be aware of how we process personal data. The only exception to this will be the following:

- Legal Advice
- Commercially Sensitive material
- Personal Data Pertaining to the Consultation Participants
- Information which would otherwise affect the operations of the MPS and is not in the public's interest to disclose.

All public requests for information should be directed to the MPS Data Protection and Freedom of Information Officer.

4. Consultation Results

1. Stakeholder Consultation:

- 1.1 Through discussion and analysis, the following potential stakeholders whose interests may need to be considered have been identified:

Stakeholders	Roles and Responsibilities	Outcomes
MPS Information Sharing Support Unit	Provision of guidance on completion of the PIA.	Advice issued and approval given
Mayor's Office for Policing and Crime	Advised full PIA required.	

- 1.2 Additional consideration has been given to other possible stakeholders; however they are not currently relevant to this process at this stage.

2. Public Consultation:

- 2.1 Public confidence in the MPS to safeguard and process all (sensitive) personal data we hold fairly and lawfully is of paramount importance to the Service. Ideally, it would have been preferable for the MPS to undertake a public consultation exercise before the pilot exercise as part of this PIA; however, the strict timescales to address the inherent need for this technology meant this was not possible.

In the absence of a full public consultation exercise before the implementation of the pilot phase, a community engagement / consultation exercise will take place post the pilot to inform the MPS position as to how this capability can / should be deployed in the MPS, and what Privacy Safeguards they legitimately expect to be in place should the decision to deploy this capability be taken.

In addition to the above, the privacy design features outlined within this document will form part of the annual review of this PIA to ensure adequacy of the protections they afford to the processing.

5. Balanced Risk Assessment

No	Risk	Likelihood L/M/H	IMPACT L/M/H	Solutions / Mitigations	Residual Risk?	MPS SIRO Sign-Off
1.	Unauthorised access to MiPS from outside of the MPS estate	L	H	MiPS is hosted within the MPS data centres, and is only accessible through a MPS internal domain. Robust corporate security procedures and firewalls protect against unauthorised access.	This is an extremely unlikely scenario. Accepted.	
2.	Unauthorised access to MiPS from within the MPS estate	L	H	MiPS access is controlled by warrant/pay number accreditation from the MPS HR system, coupled with a unique, user-set password. Users will be required to periodically change passwords for additional security. In addition, access particularly sensitive data may be controlled using restrictions and access control lists (ACLs). Full audit logs	This is an extremely unlikely scenario. Accepted.	

				are maintained of every attempt to access data, successful or otherwise.			
3.	Unauthorised interception of mobile data transmitted via public Wi-Fi or 4G	L	H	Data transmitted over non-secure networks is subject to end-to-end encryption via a MPS - approved VPN.	This is an extremely unlikely scenario. Accepted.		
4.	Loss of a MiPS-enabled mobile device	L	L	MiPS mobile devices are secured with the same security features as desktop devices within the MPS domain, and are subject to user and password authentication. In addition, a mobile device will lock when a password is tried too many times, resulting in wiping of all applications and data. Devices can also be disabled and wiped remotely. In addition, once data is transferred from a mobile device into MiPS, it is permanently cleared from the device cache.	Accepted.		

6. Implementation of PIA Outcomes Responsibilities

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved?

	Action to be taken	Date for completion of actions	Responsibility for action
1.	No action required.		
2.	No action required.		
3.	No action required.		
4.	No action required.		
Contact point for future privacy concerns Met HQ: Information Law and Security Group			

7. Conclusion

Any gathering, processing or storage of identifiable personal data introduces potential risks of data misuse and breaches of privacy. Although they can never be eliminated, such potential risks are significantly mitigated by the robust information governance controls as set out within this PIA, which are all designed to safeguard privacy. The centrality of information governance to the data, to meet or exceed all information governance standards, provides greater assurance about privacy than most organisations are able to provide.

MiPS is due to begin roll-out in April 2019 – 12 months from now.

This PIA has been produced at the express request of MOPAC, to address changes in guidance from the Information Commissioner's Office, and also to take account of the enactment of GDPR after 25th May 2018. The MPS have yet to issue guidance in relation to GDPR. Following advice from the MPS Information Sharing Support Unit (ISSU), GDPR will not materially change how the MPS uses data in relation to its statutory requirements. What the GDPR will do, is to make the completion of a DPIA mandatory for all new data processing projects. In this, MPS policy – and therefore the MiPS programme - is compliant.

However, it must again be stated that due to the extremely short timescales allowed for submission of this document, the ISSU have not been able to provide a sign-off on behalf of the MPS. This will need to be reviewed and addressed as soon as possible. Hence I have set the review time for this document at 6 months, which will then allow sufficient time for any issues raised to be robustly dealt with before the MiPS go-live date.

8. Privacy Impact Assessment Sign-off

1.	Project Sponsor / NPCC Lead
	Sign Below: Name: _____ Position: _____ Date: _____
2.	Head of Information Law and Security
	Sign Below: Name: John Potts _____ Date: _____

Appendix A

Term	Acronym	Description
Data Controller		Has the same meaning as in section 1(1) of the DPA, that is, the person who determines the manner in which and purposes for which Personal Data is or is to be processed either alone, jointly or in common with other persons
Data Protection Act 1998	DPA	Includes all codes of practice and subordinate legislation made under the DPA from time to time
Data Subject		Has the same meaning as in section 1(1) of the DPA being an individual who is the subject of Personal Data
Freedom of Information Act 2000	FOIA	Includes the Environmental Information Regulations 2004 and any other subordinate legislation made under FOIA from time to time as well as all codes of practice
Human Rights Act 1998	HRA	Includes all subordinate legislation made under the HRA from time to time
Information		Any information however held and includes Personal Data, Sensitive Personal Data, Non-personal Information and De-personalised Information. May be used interchangeably with 'Data'
Information Commissioner's Office	ICO	The independent regulator appointed by the Crown who is responsible for enforcing the provisions of the DPA and FOIA
Metropolitan Police Service	MPS	The police force for the London metropolis area (excluding the City of London)
Non- personal Information		Information that has never referred to an individual and cannot be connected to an individual.
Notification		The Data Controller's entry in the register maintained by the Information Commissioner pursuant to section 19 of the DPA
Personal Data		Has the same meaning as in section 1(1)(a) to (e) of the DPA, that is, data which relates to a living

OFFICIAL - PUBLIC

		individual, who can be identified from it, or data that can be put together with other information to identify an individual and includes expressions of opinion and intentions.
Process		Has the same meaning as in section 1(1) of the DPA and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying Personal Data
Sensitive Personal Data		The eight categories of Personal Data specified in section 2 of the DPA

Appendix C: Control page

Distribution list

Recipient	Title	Location

Change control

Version	Date	Authority	Evidence of approval	Record of change
3	29.03.2018			

